The Fort Privacy GDPR Compliance Framework

VERSION 2.0 – 25 May 2022

FORT PRIVACY
Getting Data Protection Right

www.fortprivacy.ie

Message from Fort Privacy

At Fort Privacy, we have extensive strategic, operational and technical experience in delivering successful GDPR programmes to our large and varied client base. We have used this experience to develop the Framework and we are constantly improving and refining it.

The Fort Privacy team is proud of our Framework – and rightly so!

We know that it helps us deliver real results for our clients. We also see the confidence it gives our clients as they work on their compliance programmes and how it helps their compliance improve over time.

We are delighted to share our Framework with you, to assist you in your GDPR compliance efforts. We always say that "compliance is a journey and not a destination". Think of the Fort Privacy Framework as the map for your GDPR compliance journey.

The Framework itself has 10 compliance categories, each of which is mapped to GDPR requirements. This White Paper provides a detailed explanation of each category, demonstrates how it maps to the GDPR, shows how to address the relevant category for compliance purposes and provides some case studies to illustrate how to work with it effectively.

We look forward to new challenges for our Framework including using it to assist those of our clients that are now embarking on GDPR certification journeys. We also look forward to implementing our Framework in new sectors and to adapting it to cope with some of the challenging new legislation that is being prepared at EU level.

Marie and Tricia

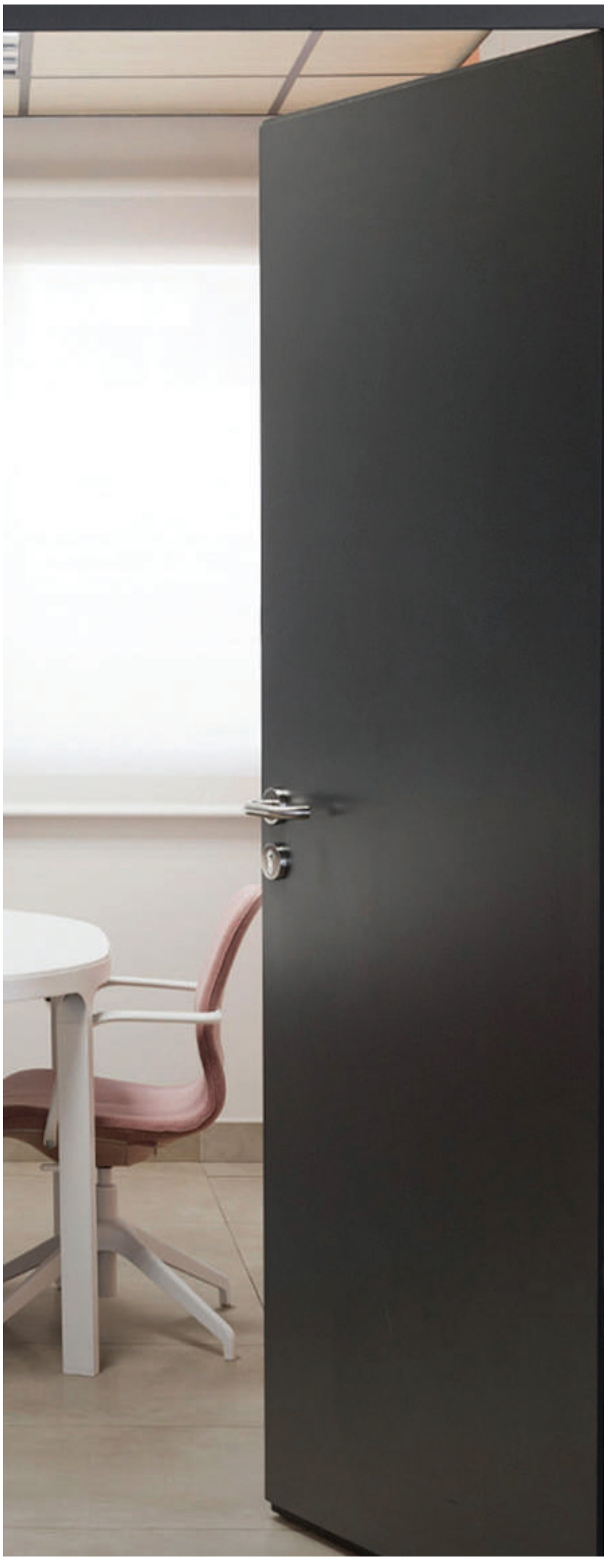
Framework Version 1.0 – 25 May 2019

Framework Version 2.0 – 25 May 2022

Table of Contents

Fort Privacy Framework Overview

1 - Introduction



Complying with data protection legislation, including the EU's General Data Protection Regulation 2016/679 ("**GDPR**") can be challenging.

The Fort Privacy GDPR Framework (the "**Fort Privacy Framework**" or the "**Framework**") will help to bring a knowledge and confidence to your GDPR compliance activities that goes far beyond mere compliance. The Framework will drive strategic goals in the business and enable the business to gain competitive advantage from compliance.

In this paper we will discuss how to use the Framework as a structure for achieving data protection compliance in an organisation.

The Fort Privacy Framework is based on the concept and structure of a maturity model framework. We will begin by explaining the concept of maturity models, how they are used and how Fort Privacy applied the principles of a maturity model to produce a Framework that ensures organisations meet their GDPR obligations.

We will break down and guide you through each category of the Framework and outline the key compliance requirements (referred to as "Criteria") under each Framework category.

We will show you how you can use the Fort Privacy Framework to remove compliance roadblocks and pave the way for achieving an optimum level of data protection compliance.

Thank you for allowing us to accompany you on your compliance journey!

WHERE IT ALL BEGAN

The GDPR formally came into effect on 25 May 2018 across the EU. As a Regulation it has direct effect in EU member states and is supported by local national law. In Ireland, the national supporting law is the Data Protection Act 2018.

The GDPR aims to modernise and harmonise Data Protection Laws across the EU/EEA to ensure they are fit for purpose in our online society. The GDPR is widely considered to be the toughest privacy and security law in the world. Since 2018 many other (non-EU) countries have introduced or upgraded their own laws to reflect some of the important concepts that are contained in the GDPR.

The GDPR is a complex piece of legislation, with 173 recitals and 99 Articles. It has two key objectives:

- Individuals who share their personal data with organisations ("data subjects") are informed about the use of their personal data and retain control over that personal data
- Organisations that process the personal data of individuals must be able to demonstrate their compliance with the GDPR across their processing activities.

The introduction of the GDPR has compelled many organisations to view data protection compliance as a key function of the organisation, requiring concrete resources such as dedicated teams and reporting structures.

We formed Fort Privacy to help organisations successfully manage their GDPR compliance. We realised early on that the effective, development, implementation and management of an organisation's data protection programme is critical to its success and that this demands a structure and focus to compliance activities. Based on this realisation, we started to develop the Fort Privacy Framework, utilising Maturity Models such as AICPA/CICAs Privacy Maturity Model.

Over time, the Framework has become our focal point for delivering our GDPR compliance services to such an extent that it is difficult to imagine how we would deliver services effectively without it.

The Fort Privacy Framework facilitates us in effectively supporting our clients in successfully managing their risk and compliance efforts as it can be used both to assess their risk profile and set compliance priorities based on that profile. Once their GDPR compliance programme is in place, many of our clients continue to use the Framework as a tool for ongoing strategic and accountable data protection compliance.

We know that we will continue finding new ways to develop the Framework and apply it for the benefit of all our clients.

(see Fort Privacy Case Studies).

2 - Maturity Models and the Framework

INTRODUCING MATURITY MODELS

Maturity Models are not a new concept and have long been used by industry to measure the ability of an organisation to continuously improve in a discipline.

The most famous of these models, the Capability Maturity Model (CMM) from the Software Engineering Institute (SEI)—a model that was initially developed to measure the maturity of software development practices—first emerged in 1987. The CMM model has become the standard for measuring capabilities in the software development industry, which generally embraces standards quickly, and the structure of the CMM has been reused for the development of many other maturity models.

A maturity model can be viewed as a set of structured levels that describe how well the behaviours, practices and processes of an organisation can reliably and sustainably produce required outcomes. A maturity model can be used to evaluate performance and to guide performance improvement.

Caralli et al. define a maturity model as "a set of characteristics, attributes, indicators or patterns representing progress in a particular domain or discipline. These models help organisations to evaluate and benchmark their practices, processes and methods against a clear set of standards or best practices of the given domain or discipline. Organisations can apply maturity models to define their current level of maturity and then determine the expected path of improvement."

Maturity models use levels to assess an organisation's level of maturity and allow them to attain high standards over time. The aim is to achieve the optimised level of maturity.

HOW THE FORT PRIVACY FRAMEWORK USES MATURITY MODELS

Fort Privacy has taken the traditional maturity model structure and adapted it for use by organisations to structure and evidence how they comply with their data protection obligations under the GDPR.

The Framework brings much needed structure to data protection programmes and provides a way to measure their effectiveness by working through 10 categories of compliance, which we have identified as essential to achieving compliance under the GDPR. The Framework facilitates a risk based and proactive approach to compliance.

FORT PRIVACY FRAMEWORK - LEVELS OF MATURITY

Maturity Models define a five-level progression path to measure and guide organisations on the road to achieving data protection compliance:

LEVEL 1 (AD-HOC)

At this level, the organisation has minimal, or no compliance activities undertaken to achieve compliance. There is not enough documentation to enable any level of success or adherence to the requirements of the GDPR.

LEVEL 2 (DEFINED)

The organisation has at the very least documented the requisite procedures and processes that form part of its data protection programme.

LEVEL 3 (IMPLEMENTED)

The organisation has implemented and adopted the documented procedures and processes.

LEVEL 4 (MEASURED)

The organisation has sought to assess the effectiveness of the adopted procedures and processes.

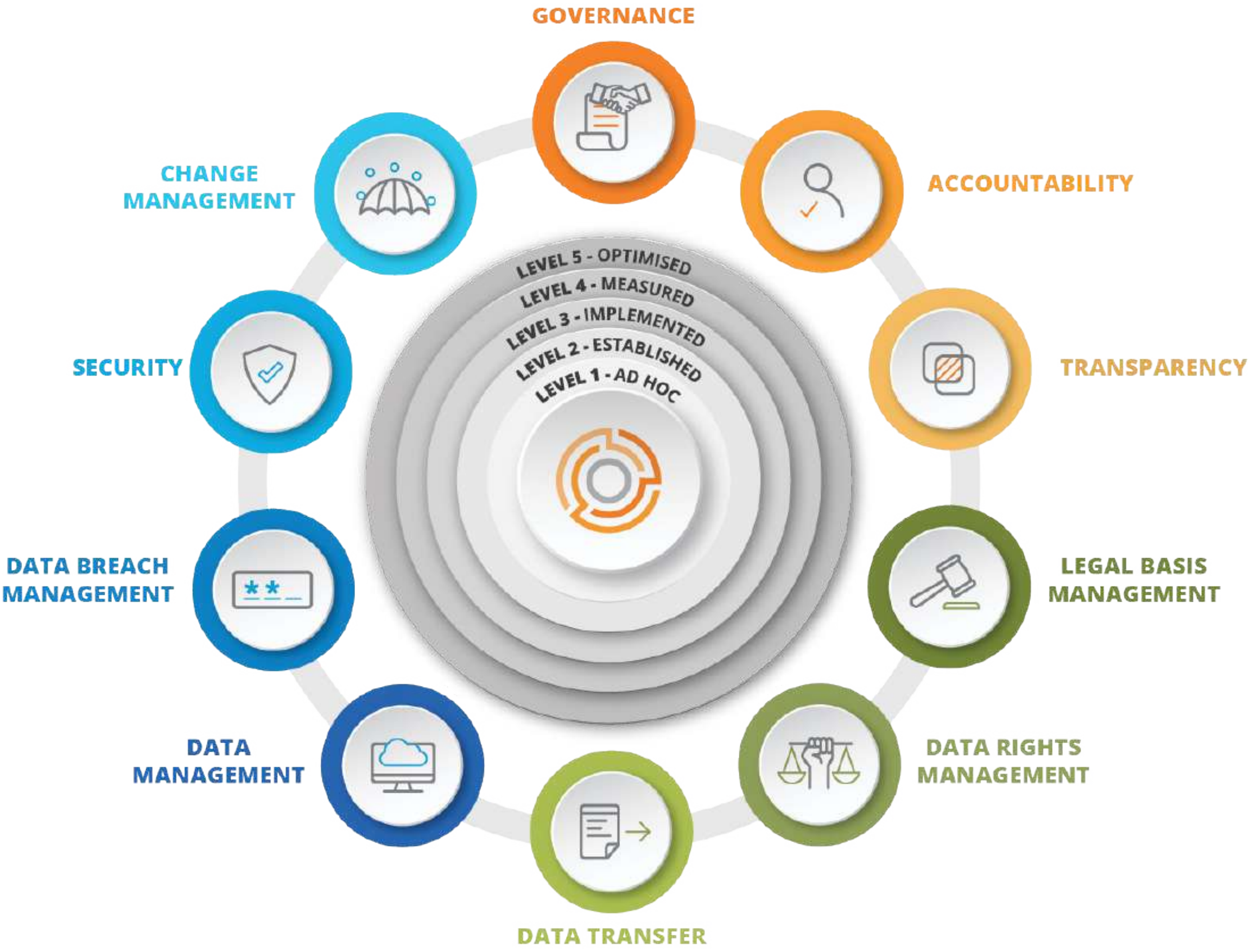
LEVEL 5 (OPTIMISED)

The organisation is using the assessments to proactively address and improve its procedures and processes.

3 - The Framework Categories

The Fort Privacy Framework simplifies compliance with the GDPR by categorising the main requirements under 10 compliance categories. The categories are as follows:

FRAMEWORK CATEGORY	DESCRIPTION
GOVERNANCE	The organisation defines a structure and policy for decision making, accountability and control with clearly defined roles and responsibilities for data protection compliance.
ACCOUNTABILITY	The organisation can account for all its data processing activities and demonstrate compliance with relevant laws.
TRANSPARENCY	The organisation informs all affected data subjects about its processing activities and communicates the purposes for which personal data is processed.
LEGAL BASIS MANAGEMENT	The organisation identifies a reliable Legal Basis for each processing activity and ensures all processing activities are consistent with the identified legal basis.
DATA SUBJECT RIGHTS MANAGEMENT	The organisation implements policies and processes to facilitate and respond to data subjects who exercise their rights under the GDPR.
DATA TRANSFER MANAGEMENT	The organisation discloses personal data outside the organisation (to third parties or via intra-company transfers) using valid legal mechanisms and appropriate safeguards.
DATA MANAGEMENT	The organisation manages personal data processing activities to ensure consistency with the principles of purpose limitation, data minimisation, accuracy and storage limitation.
DATA BREACH MANAGEMENT	The organisation implements policies and procedures to appropriately manage and respond to personal data breaches.
SECURITY	The organisation implements technical and organisational measures to manage the security of personal data and of the systems that it uses to process the personal data.
CHANGE MANAGEMENT	The organisation ensures that it manages changes to personal data processing activities to ensure ongoing compliance.


GOVERNANCE
ACCOUNTABILITY
TRANSPARENCY
LEGAL BASIS MANAGEMENT
DATA RIGHTS MANAGEMENT
DATA TRANSFER
DATA MANAGEMENT
DATA BREACH MANAGEMENT
SECURITY
CHANGE MANAGEMENT
LEVEL 5 - OPTIMISED
LEVEL 4 - MEASURED
LEVEL 3 - IMPLEMENTED
LEVEL 2 - ESTABLISHED
LEVEL 1 - AD HOC

4 - How does the Framework Help?

Organisations struggle 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 externally, against other similar organisations.

By breaking down the obligations of the GDPR into a set of clear, measurable deliverables, the Fort Privacy Framework provides a structured roadmap for organisations to achieve GDPR compliance.

The Fort Privacy Framework allows organisations to:

- structure compliance activities,
- assess progress,
- prioritise important areas that need work and improvement,
- create work plans,
- achieve measurable results, and
- demonstrate compliance.

The importance of identifying a clear and structured approach to a data protection compliance programme has never been more necessary. The scope of compliance requirements is getting more and more complex as the full remit of the GDPR comes into play.

There is an increasing requirement for organisations to move away from basic data protection compliance structures and build a culture of compliance as a key part of their business strategy. (see Fort Privacy blog 'Beyond GDPR compliance').

The Framework facilitates the journey from ad hoc to strategic compliance by providing a 10 Category structure and 5 levels of maturity. An Organisation can manage its compliance progression category by category through the maturity levels ensuring it is setting manageable and achievable objectives.

As we work through the Framework with our customers it has become increasingly clear how the interplay between each category operates. Compliance is like a big jigsaw puzzle that comes together overtime and unless you have all the pieces it's impossible to get the full picture.

No one category will bring compliance to an organisation in of itself. Each category is linked to other categories in the Framework. While some categories may be more important than others in the context of the relevant organisation, it will be necessary to go through the Framework from start to finish to get a full overview of compliance requirements.

The Framework is cyclical and our general approach is to work through all the categories over a 12-month period. It's often only on the third or fourth round of the Framework that an organisation will really feel the full effect of embedding a Framework into their organisation in terms of compliance maturity and, in many cases, increasing their commercial proposition.

Fort Privacy Framework by Category

Category 1 - Governance

The organisation defines a structure and policy for decision making, accountability and control with clearly defined roles and responsibilities for data protection compliance.

1. GOVERNANCE - OVERVIEW

Good Governance is key to an organisation's compliance programme. An organisation must assign roles and responsibilities to meet compliance requirements.

Every organisation should appoint a person with responsibility for data protection compliance activities. Many organisations will be legally required (or may choose) to appoint a Data Protection Officer ("DPO") and will need a Data Protection Team in place to ensure that compliance requirements are met. Some larger organisations may need to make Data Protection a function in the organisation.

Data Protection Teams should meet regularly to progress the compliance programme. Regular reporting to board or management teams is necessary for good Governance. Governance activities also include ensuring the registration requirements of Supervisory Authorities across the EU are met where relevant.

Organisations should firstly review and evaluate their governance structures against the criteria listed below, to ensure that the right structures are in place.

Documentation of all roles and responsibilities is key with a structured and regular approach to meetings and reports. A documented Governance Policy will be the right solution for many organisations. An organisation may also need to review and document its role under the GDPR, as joint controller, controller or processor.

Without good governance it is unlikely the organisation will be successful in meeting compliance requirements.

2. GOVERNANCE - GDPR ARTICLES

The relevant GDPR articles are:

- **Article 5** - Principles relating to processing of personal data
- **Article 24** - Responsibility of the controller
- **Article 26** - Joint controllers
- **Article 37** - Designation of the data protection officer
- **Article 38** – Position of the data protection officer
- **Article 39** - Tasks of the data protection officer

3. GOVERNANCE - CRITERIA

(a) Roles & Responsibilities

Organisations should consider, and document, the appropriate governance structure based on their compliance requirements under the GDPR. There should be a clear and documented policy for how the organisation will resource its GDPR compliance activities, from the management team to DPO/DP Lead, Data Protection Teams and members of staff. Everyone has a part to play and it's important that everyone understands what their role is and is equipped to fulfil it. Organisations must also consider their role under the GDPR as controller/joint controller/processor and in some cases will benefit from formally documenting the analysis around this, particularly where there may be challenges raised.

(b) Designation of DPO/Data Protection Lead

The Data Protection Lead/DPO is a key role in the organisation. If there is a legal requirement under the GDPR to appoint a DPO (or the organisation self-appoints) that should be clearly documented. A decision not to appoint a DPO should also be documented in some cases and especially where there is some ambiguity as to whether the appointment of a DPO is legally required or not. EDPB guidance should be used to inform this decision.

(c) Role of DPO

The GDPR formally defines the position of the DPO at Article 38. It states that resources must be provided to the DPO to carry out its role effectively and the organisation must be able to demonstrate that this is the case. Once appointed, organisations must ensure that the DPO is involved 'properly and in a timely manner" in all matters concerning data protection. The DPO must also be properly supported with tools and resources (including training) to fulfil the requirements of the role. It should be noted that the requirements of Article 38 are relevant for both controllers and processors.

In many organisations it is advisable to appoint a Data Protection Team to support the DPO/Data Protection Lead to ensure the requirements of the GDPR can be met. The Data Protection Team will support the DPO and ensure the DPO is fully informed about processing activities in the organisation.

(d) Reporting

Article 38 of the GDPR states that the DPO should "directly report to the highest management level". Organisations should have formal reporting structures in place to facilitate such reports. Management/board reports should be documented to demonstrate compliance. Progress in key areas, risks and issues should be reported by the DPO. The management team should be trained to understand reports received so that the right tools and resources are in place to address gaps identified. Regular communications should be undertaken to ensure that staff understand reporting structures so that issues such as breaches or changes in processing activities are reported up as required.

(e) Registration with Supervisory Authority and Guidelines

Organisations need to ensure appropriate registrations are undertaken with the relevant Supervisory Authority. In Ireland, all organisations that have appointed a DPO, pursuant to Article 37(1) GDPR, are required to notify the contact details of their DPO to the Irish Data Protection Commission ('**DPC**'). The DPC maintains these details in a Data Protection Officer Register.

Organisations with entities in various EU countries may need to ensure that the in-country Supervisory Authority registration requirements are met for each country. Organisations need to be aware of updates, advice and guidance that is communicated from Supervisory Authorities and the EDPB. As part of its Governance activities, each organisation should keep abreast of the ever-changing data protection landscape to ensure that it adopts the most relevant guidance for its industry.

4. GOVERNANCE - FORT PRIVACY CASE STUDY

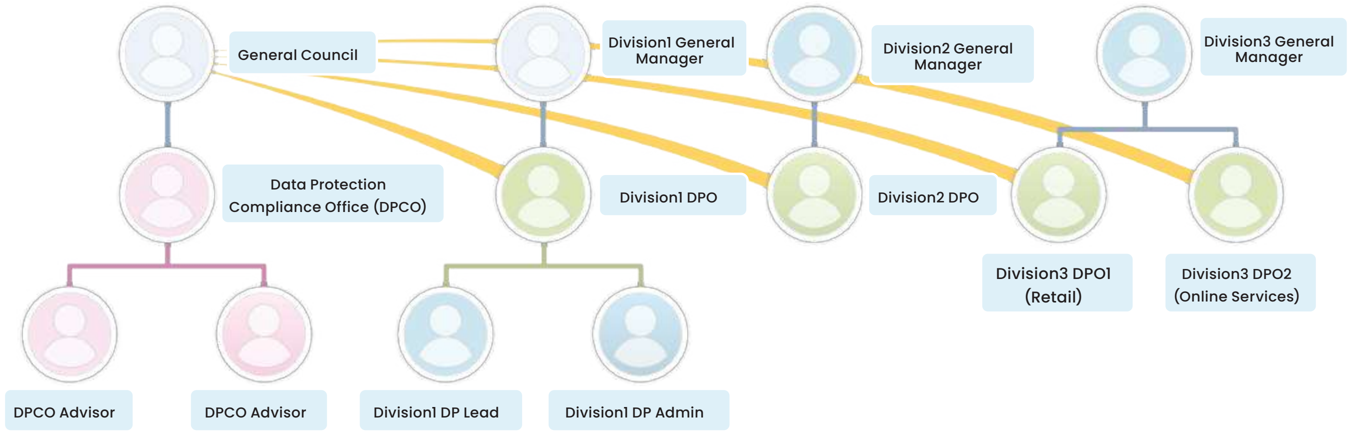
Client / Organisation: Large multinational

Over the course of a number of years, Fort Privacy worked on a strategic project with an organisation with a large corporate structure. The aim of this project was to ensure that the organisation's governance structure was equipped to handle the diverse scope of its processing operations.

By utilising the Fort Privacy Framework to structure all compliance activities the organisation was able to put in place a consistent approach to data protection compliance. This approach has allowed 5 Data Protection Officers (with supporting Data Protection Teams) and a central Data Protection Compliance Office function to consistently manage the strategy and oversight of its compliance activities.

Company DP Compliance

Illustrating DPCO Role Reporting Lines for DPOs


General Council
Division1 General Manager
Division2 General Manager
Division3 General Manager
Data Protection Compliance Office (DPCO)
Division1 DPO
Division2 DPO
Division3 DPO1 (Retail)
Division3 DPO2 (Online Services)
DPCO Advisor
DPCO Advisor
Division1 DP Lead
Division1 DP Admin

5. GOVERNANCE - MATURITY MODEL APPLICATION

When applying a maturity model approach an organisation should assign and document appropriate roles and responsibilities in the organisation to address compliance requirements. Level 4 or Level 5 maturity in the Governance category requires an organisation to have a strong data protection culture with top level buy-in ensuring sufficient resources and tools to facilitate compliance. Regularly reviewing resource requirements and training and ensuring issues are being addressed will reflect strong adoption of the GDPR across the organisation. Maintaining good Governance in an organisation provides a solid foundation for compliance across the other categories.

The table below defines Level 1 to 5 for each Governance Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Roles & Responsibilities The organisation has documented roles and responsibilities that demonstrate commitment to data protection compliance activities.	Roles & responsibilities exist informally but may not be complete or may not have senior management commitment.	Roles & responsibilities are fully documented.	Roles & responsibilities are defined and fully implemented.	Roles & responsibilities are measured and reviews are conducted to assess their effectiveness.	Roles & responsibilities are proactively managed for optimisation. Issues are identified, and remedial action taken to address them in a timely manner.
Role as Controller/Processor The organisation has documented its role under the GDPR (as controller, joint controller, processor) for all relevant processing activities and meets relevant compliance requirements for that role.	No formal consideration has been given to the role of the organisation.	The role of the organisation is fully documented for all processing activities.	Consideration has been given to the role of the organisation and key compliance requirements are met for the relevant role identified.	The organisation proactively assesses its role to ensure conformity	The organisation seeks ways to improve understanding in the organisation of the requirements of the role (as controller/processor/ joint controller) Changes are made as required.
Designation of a DPO/DP Lead A DPO/DP Lead has been appointed to implement and support Data Protection compliance activities.	DPO/DP Lead is not appointed formally or is appointed in name only. DPO/DP Lead is allocated on an "as needed" basis to address DP issues as they arise.	DPO/DP Lead is formally in place; however, they may not have appropriate resources, training or skillset. Maybe conflict with role.	DPO/DP Lead is in place and is empowered with appropriate authority and resources and has the right qualifications.	The organisation ensures that an adequately qualified DPO/DP Lead is identified and made available throughout the organisation to support its various privacy initiatives. The effectiveness of the appointment is measured.	The organisation reviews the DPO/DP Lead function and seeks ways to improve skill set and knowledge base, including assessing the adequacy, availability and performance of the DPO/DP Lead. Changes are made as required.
Role of DPO The DPO role is undertaken in compliance with the requirements of the law.	DPO role is not, or is only partly, being undertaken in compliance with the law.	A DPO is formally in place; however, there may be conflict with role or may not be undertaking all requirements of the role.	DPO is empowered and the role is being undertaken in compliance with the law.	The organisation reviews and measures the effectiveness of the role of DPO.	The organisation reviews the DPO role and seeks ways to develop the role, including assessing the adequacy, availability and performance of the DPO. Changes are made as required.
Reporting Structures The organisation has effective reporting structures to meet its compliance requirements. Regular communications with staff are in place to ensure issues are reported to DPO/DP Lead.	Limited, if any reporting activity is undertaken in the organisation.	Clear reporting lines and reporting requirements are identified in the organisation.	Reporting lines and reporting requirements are undertaken in accordance with the documented reporting policy.	Reporting activity is measured to assess its effectiveness.	The organisation reviews its reporting requirements and seeks ways to increase awareness and understanding of reports provided. Issues identified in reports are actioned.
Registration with Supervisory Authorities and Guidelines The organisation meets supervisory authority registration requirements and keeps up to date with relevant data protection guidelines.	Registration is not undertaken as required and guidelines are not reviewed or adhered to.	Registration is undertaken but may not be maintained. Guidance is reviewed.	All relevant registration requirements are met, documented and maintained. Relevant guidance is implemented as required.	Reviews are undertaken to ensure all relevant guidelines and registrations are uptodate and maintained.	The organisation makes changes as required to adopt any findings from reviews undertaken.

Category 2 - Accountability

The organisation can account for all its data processing activities and demonstrate compliance with the requirements of the GDPR.

1. ACCOUNTABILITY - OVERVIEW

Representing one of the foundational principles of the GDPR, accountability requires organisations to show the measures taken to ensure compliance with the GDPR, as well as the effectiveness of these measures.

Accountability has some of the most challenging compliance requirements as it requires logging, tracking and auditing activities across all aspects of data processing in the organisation in order to achieve compliance.

Accountability encompasses a wide range of activities that are monitored and tracked over time and cannot be achieved without dedicated and ongoing effort. Organisations that wish to demonstrate compliance with the accountability principle must dedicate appropriate resources to the task. Organisations will need to build evidence of the steps taken to remain accountable under GDPR, such as ensuring all staff are adequately equipped with an understanding of the requirements of the GDPR, regularly auditing activities and maintaining up-to-date Records of Processing Activities.

The first steps on the journey to achieving compliance maturity under the accountability category is to document policies and procedures and build a Record of Processing Activities. Demonstrating that the organisation is working to a defined data protection programme, such as the Fort Privacy Framework, is also a sure way of demonstrating compliance with the accountability requirements.

Any changes or cessation of processing activities will need to be captured in the Record of Processing Activities to ensure it continues to accurately reflect the organisation's processing activities. Implementing mitigation actions to counter the key risks identified by the organisation, as well as offering regular awareness training to staff are also hallmarks of organisations who are serious about their accountability compliance requirements.

2. ACCOUNTABILITY - GDPR ARTICLES

- **Article 5** - Principles relating to processing of personal data
- **Article 24** - Responsibility of the controller
- **Articles 12-23** - Rights of the data subject
- **Article 30** - Record of processing activities
- **Article 38** – Position of the data protection officer
- **Article 39** - Tasks of the data protection officer
- **Article 40** – Codes of conduct
- **Article 42** - Certification

3. ACCOUNTABILITY - CRITERIA

(a) Data Protection Policies and Procedures

The GDPR requires that organisations implement technical and organisational measures to ensure that the safety and integrity of personal data is maintained. The Data Protection Policy is the foundation of all data protection compliance activities. As a key policy in the organisation, this document along with other Data Protection related policies should clearly set the tone by defining a policy for compliance. Certain data protection policies will need to be backed up with procedures demonstrating how the policy is implemented operationally in the organisation. All members of staff should be required to review and acknowledge policies and procedures and training should be provided to relevant individuals to ensure these are implemented correctly.

(b) Record of Processing Activities

From an external regulator's perspective, the Record of Processing Activities ("**ROPA**") represents the keys to the kingdom. This is a detailed record of each processing activity undertaken in the organisation including, the legal basis for processing, type of personal data processed, transfers undertaken and summary of technical and organisational measures. Whether the organisation is a controller or processor (or both) will determine how much information is required to ensure the ROPA complies with Article 30 of the GDPR.

The ROPA is an important accountability step as supervisory authorities, such as the Data Protection Commission in Ireland, may request that an organisation produces a ROPA when undertaking an audit or investigating a breach. A well-documented ROPA is hugely beneficial to an organisation as it provides key information about its processing activities. If time and attention is given to documenting the ROPA properly and owners are assigned to ensure it is maintained, the ROPA can be a powerful document setting the scene for all compliance activities in the organisation.

(c) Logs of Data Protection Activities

Maintaining logs is a simple and effective way for an organisation to reflect accountability and demonstrate ongoing compliance with the GDPR. Data Protection Activity log(s) should be updated to reflect the status of data protection and data processing activities and incidents. It is crucial that organisations treat this as a live document or series of documents as appropriate to the size and complexity of the organisation.

Logs should be continuously maintained. Examples of the types of logs that might be maintained are logs of meetings and reports, project plan tasks, breach logs, DPIA logs, DSAR logs and supplier logs.

(d) Data Protection Risk Register

Organisations need to acknowledge the inherent risks associated with accumulating and storing personal data. By documenting these via a Risk Register, an organisation can demonstrate the steps it has taken to comply with the accountability principle under the GDPR. A Data Protection Risk Register identifies the key risks of the organisation. To ensure full compliance, it is not enough to simply identify a list of risks, the organisation must also specify the mitigation actions it has taken and be able to demonstrate its progress against those actions. Key risks should be reported to the management team/board on a regular basis.

(e) Training

Ensuring staff are properly trained and aware of their responsibilities under GDPR represents some of the strongest evidence an organisation can provide of its compliance measures. By raising awareness amongst staff, organisations can minimize the risk of an event such as a breach occurring.

Data Protection is a specialised field, and an organisation should not expect staff to be fully aware of their obligations without some formal training. The obligation to provide training is also specifically mentioned as one of the tasks of a DPO under Article 39 GDPR. Training should be undertaken at least annually and can be conducted in multiple ways such as in person workshops or via e-learning platforms. Evidence of the training undertaken should be maintained including any tests/accreditations.

(f) Audit and Certification

Important actions an organisation can take to demonstrate accountability include actively working towards implementing and maintaining appropriate internal and third-party audit programmes and certifying to data protection relevant standards where appropriate. Audit programmes should cover all relevant processing activities and should be fully documented in case the organisation is requested to provide evidence of the accountability measures it has taken.

Organisations should also look to identify relevant certifications and develop a certification strategy. Commitment to certification requires an appropriate budget and resources and is a long term strategy for an organisation. An organisation should ensure that it has evidence that it is maintaining its certification(s) in the event it has already acquired one.

4. ACCOUNTABILITY - FORT PRIVACY CASE STUDY

Client /Organisation: Multinational Company

Fort Privacy engaged with an organisation which sought to revamp how it approached its compliance activities. Using the Fort Privacy Framework as the foundation for its strategy, the organisation sought to develop a greater understanding of how data flowed across the various business units by undertaking a data mapping exercise.

The organisation was able to organise, categorise, manage and structure data for its operational requirements. By completing an in-depth analysis of the data journey across the organisation, it was able to identify gaps in its processes which needed to be addressed. This data mapping exercise provided a solid basis for the organisation to build on when it came to documenting the record of processing activities (ROPA) at a later stage.

The result of this project was that the organisation successfully developed an extensive record of the different types of information flows within the group. It also provided the organisation with evidence of the steps it had taken to ensure compliance with the GDPR.

5. ACCOUNTABILITY - MATURITY MODEL APPLICATION

When applying a maturity model approach to the Accountability category, an organisation should document its data protection policies and procedures and its record of processing activities and ensuring an appropriate training programme is in place. Level 4 or Level 5 maturity in the Accountability category requires audits and risk management to be at the fore front of activities along with regular review and update of compliance materials.

The table below defines Level 1 to 5 for each Accountability Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Data Protection Policies and Procedures The organisation's Data Protection policies and procedures include provisions to enable the organisation to demonstrate compliance with data protection requirements.	Some aspects of the Data Protection policies & procedures exist informally.	Data Protection policies and procedures exist and are fully documented.	Data Protection policies and procedures are defined and implemented.	Compliance with Data Protection policies and procedures are measured and reviews are conducted to assess the effectiveness of the controls in place.	The organisation monitors compliance with Data Protection policies and procedures proactively to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
(CONTROLLER) Record of Processing Activities (ROPA) All Controller related data processing activities are documented in a ROPA that meets the requirements of Article 30 of the GDPR.	The identification of and documentation of Controller related processing activities is irregular, incomplete, inconsistent, and potentially out of date.	The ROPA has been documented for all material Controller related processing activities	All Controller related processing activities have been documented with owners assigned. The organisation regularly reviews and maintains the Controller ROPA to ensure it is kept current	Procedures exist to monitor compliance of the Controller ROPA. The Controller ROPA is used proactively to ensure that Data Protection policies and procedures are in line.	The Controller ROPA is used as a tool to monitor compliance in the organisation and identify key gaps and risks. Issues are identified and compliance activities are undertaken as a result.
(PROCESSOR) Record of Processing Activities All Processor related data processing activities are documented in a ROPA that meets the requirements of Article 30 of the GDPR.	The identification of and documentation of Processor related processing activities is irregular, incomplete, inconsistent, and potentially out of date.	The ROPA has been documented for all material Processor related processing activities.	All Processor related processing activities have been documented with owners assigned. The organisation regularly reviews and maintains the Controller ROPA to ensure it is kept current.	Procedures exist to monitor compliance of the Processor ROPA. The Processor ROPA is used proactively to ensure that Data Protection policies and procedures are in line.	The Processor ROPA is used as a tool to monitor compliance in the organisation and identify key gaps and risks. Issues are identified and compliance activities are undertaken as a result.
Activity Logs Data Protection Activity Logs are actively maintained in the organisation to ensure that key activities are captured.	Creation and maintenance of Activity Logs is informal, inconsistently applied and incomplete.	Activity Logs are in place and fully documented for all material aspects.	Activity Logs are actively reviewed and managed in the organisation.	Activity logs are monitored and their effectiveness tested to support ongoing compliance.	The organisation analyses and monitors compliance results from ongoing maintenance of Activity Logs and makes adjustments to fill gaps identified.
Training The organisation actively works towards implementing and maintaining an appropriate training and awareness programme for all staff in the organisation.	No formal training programme is in place or training is inconsistent/not appropriate.	Training needs are formally identified and a training and awareness programme is in place and fully documented for all material aspects.	The training and awareness programme is fully resourced, training is rolled out to all staff and awareness measures are implemented.	The organisation monitors and measures the effectiveness of training and awareness activities to ensure the organisation's training and awareness programme support its compliance requirements.	The organisation analyses and monitors results of compliance activities and ensures the organisation's training and awareness programme is adjusted to meet evolving training and awareness needs.
Data Protection Risk Register A risk register is used to establish a risk baseline and to identify new or changed risks in processing activities and to develop and update risk mitigation activities.	Limited, if any, formal risk identification activity is undertaken. The risks identified are incomplete and inconsistent.	All material risks are documented as part of a formal risk programme.	Processes have been implemented for risk identification, risk assessment and reporting. A documented framework is used, and risk appetite is established.	Risks are reviewed both internally and externally. Risk management is reviewed regularly.	A formal risk management review is undertaken to assess the effectiveness of the programme and changes are made where necessary.
Audit and Certification The organisation actively works towards implementing and maintaining an appropriate internal and third party audit programme as appropriate and certifies to data protection relevant standards where appropriate	Creation and review of audit programme is informal, inconsistently applied and incomplete. Commitment to certification (if relevant) is ad hoc and not part of organisational strategy.	Audit programme is in place and is fully documented for all material aspects. Relevant certifications have been identified and the organisation has outlined its certification strategy.	An audit programme is fully implemented and regular audits are carried out. A certification programme is fully implemented and maintained for all relevant products/services.	The organisation monitors and measures activities to ensure the organisation's audit/certification programme addresses relevant data processing activities taking into account processing risks and changes in process activities.	Management analyses and monitors results of compliance reviews of the organisation's audit and certification programme and proactively initiates remediation efforts to ensure ongoing and sustainable compliance. Certifications are renewed at appropriate intervals and maintained to the most up-to-date versions.

Category 3 - Transparency

The organisation informs all affected data subjects about its processing activities and communicates the purposes for which personal data is processed.

1. TRANSPARENCY - OVERVIEW

Transparency requires clear information to be provided to the data subject about the way their personal data is being used by the organisation. The GDPR is very prescriptive about the information that should be provided to data subjects regarding the processing of their personal data.

The European Data Protection Board describes Transparency as 'an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights.'

When collecting personal data, an organisation must provide clear information at initial touch points with the data subject. This feeds into information provided in notices, on forms (hardcopy and e-forms) and on websites where personal data is collected. Transparency also feeds into other complex areas such as cookies and tracking activity, and the use of CCTV.

To be compliant organisations must ask themselves two key questions:

- Am I telling the data subject everything that they should be told (in compliance with Articles 13 and 14 GDPR)?
- Am I giving this information to the data subject at every touchpoint that I have with them?

2. TRANSPARENCY - GDPR ARTICLES

The relevant Transparency articles in the GDPR are;

- **Article 5** - Principles relevant to processing of personal data modalities for the exercise of the rights of the data subject
- **Article 12** - Transparent information, communication and modalities for the exercise of the rights of the data subject
- **Article 13** - Information to be provided where personal data are collected from the data subject
- **Article 14** - Information to be provided where personal data have not been obtained from the data subject
- **Article 26** - Joint controllers

3. TRANSPARENCY - CRITERIA

(a) Provision of Data Protection Statements

Key to transparency requirements under the GDPR is the requirement to ensure that organisations provide a data protection statement that is readily available to all relevant data subjects and that reflects information about the processing activities undertaken. A data protection statement is an important way to help individuals make informed decisions about whether to provide personal data to an organisation and ensure their rights are protected.

Organisations must provide the data subjects with accurate, clear and complete data protection statements to ensure there is no ambiguity around the processing activities undertaken

A GDPR compliant data protection statement should include at a minimum the following:

- Contact details of the controller and DPO/DP Lead
- The purpose of processing
- The categories of personal data
- The recipients of the personal data
- Safeguards in place for cross boarder transfers
- Retention periods
- The legal basis and (if applicable) the legitimate interest pursued
- The rights of the data subject
- Details of any automated decision making
- The right to withdraw consent and how to exercise that right
- The right to lodge a complaint

(b) Presentation of Data Protection Statements

While the content of data protection statements is important, an organisation must also consider how and when to provide the notice to impacted data subjects.

Notice should be provided to the data subject in a timely manner:

a) at or before the time personal data is collected, or as soon as practical thereafter;

b) at or before the organisation changes its processing activities, or as soon as practical thereafter; or

c) before personal data is used for new purposes not previously identified.

Accessibility to the relevant information should be considered. This requires information to be presented in clear language and made available in a variety of formats/media conducive to the accessibility options of all applicable data subjects.

Best practice is to provide information in layered format allowing immediate access to high level summary information with more detail accessible to the data subject if required.

(c) Communication of Data Protection Statements

Organisations need to identify all scenarios where personal data is collected and data protection statements should be presented to the data subjects at these collection touchpoints, so the data subjects are fully informed in a timely manner about how the organisation will process their personal data and on what legal basis.

This requires organisation to conduct on-going monitoring to ensure its data protection statement is presented where necessary for easy accessibility by the data subject.

(d) Websites and Cookies

Websites that users interact with can be very heavy processors of personal data of those individuals. Some of this is obvious such as direct collection of data through online forms that the user completes. Other data collection is less visible to the user such as the use of cookies and similar tracking technologies.

The requirements governing the use of cookies and tracking technologies are split between the GDPR and the ePrivacy Directive. It is an important part of these requirements that the data subject is fully informed about an organisation's use of cookies and can exercise their consent to the use of certain cookies where consent is required.

4. TRANSPARENCY - FORT PRIVACY CASE STUDY

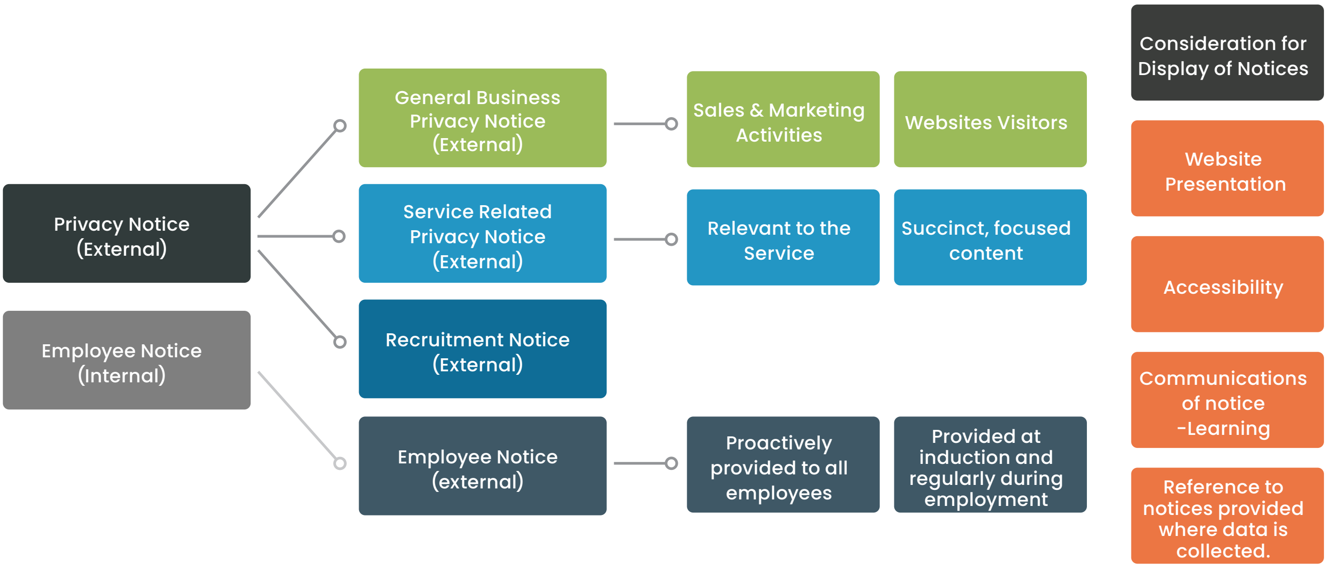
Client / Organisation: Multinational Financial Services Company

We helped a global financial services company to redraft its Data Protection Statement to meet the requirements of Articles 12-14 of the GDPR. Prior to the redraft, the organisation had two data protection notices – one internal aimed at employees and one external aimed at all other data subjects with whom the company interacted, comprising a myriad of different cohorts of people including suppliers, corporate clients, prospective clients, website visitors, users and job applicants. The external notice, in attempting to address everyone at once, ended up addressing no-one adequately.

The company delivers complex services to millions of users globally and the relevant Notice also needed to address users in multiple locations.

We split the notice into four individual notices, addressing respectively; i) job applicants, ii) clients, suppliers and website visitors, iii) the global user base and iv) employees. The notice addressing the company's service users includes sections addressing users in each location where the company does business.

The split enables the company to present relevant information when interacting with each cohort of users. Importantly, it demonstrates a confidence in the company's approach to data protection which is visible to their existing and prospective clients.


Privacy Notice (External)
Employee Notice (Internal)
General Business Privacy Notice (External)
Service Related Privacy Notice (External)
Recruitment Notice (External)
Employee Notice (external)
Sales & Marketing Activities
Websites Visitors
Relevant to the Service
Succinct, focused content
Proactively provided to all employees
Provided at induction and regularly during employment
Consideration for Display of Notices
Website Presentation
Accessibility
Communications of notice -Learning
Reference to notices provided where data is collected.

5. TRANSPARENCY - MATURITY MODEL APPLICATION

Achieving the first levels of maturity in this category requires clear information to be provided at initial touch points with the data subject when personal data is being collected. Level 4 and Level 5 maturity will come when all relevant information is maintained on a regular basis and particularly when processing activities change in the organisation.

The table below defines Level 1 to 5 for each Transparency Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Provision of Notice Notice(s) is provided to the data subject that include a complete description of the processing activities of the organisation.	Notices are informal, omit some required information about processing activities.	Notices are formally documented but may not be maintained.	Notices contains complete and relevant information in plain and simple language, appropriately labelled, easily accessible.	Notices are reviewed periodically to ensure content is kept up-to-date and accurate and new sections(layers) are developed to document new processing activities where appropriate.	A formal change management process is in place to ensure that updates to Data Protection Notices are considered for every project undertaken.
Presentation of Notice Key information is provided to the data subject (a) at or before the time personal data is collected, or as soon as practical thereafter, (b) at or before the organisation changes its Data Protection Policies and procedures, or as soon as practical thereafter, or (c) before personal data is used for new purposes not previously identified. Relevant information is presented in clear language and made available in a variety of formats/media conducive to the accessibility options of all Data Subjects.	Data Protection Notice may not be readily accessible nor provided on a timely basis.	Data Protection Notices are provided to Data Subjects but may not be provided in all cases when personal data is collected or where data is used for new purposes.	Data Protection Notices are documented, readily accessible and made available whenever Personal Data are collected, provided in a timely fashion and clearly dated. Updates are communicated when changes are made. Data Protection Notices that are provided electronically are easy to access and navigate.	A periodic review of all sources of Personal Data is carried out to ensure continued timely presentation of the Data Protection Notice in all cases where Personal Data are collected. The effectiveness of notice provided is measured.	A formal change management process is in place to ensure that every project undertaken formally ensures updated notices are provided in a timely manner to impacted data subjects and that any changes impacting existing data collection is proactively communicated.
Communication of Notice: Links to the Data Protection Notice(s) and relevant summary information where appropriate is embedded in forms and screens where personal data is collected across all forms of communication with the data subject including, documents, applications, notices, social media accounts, verbal, etc. ("Communication Forms").	A Data Protection Notice is available on the organisation's website but no attempt is made to proactively communicate the notice to the Data Subject during engagements.	A Data Protection Notice is not consistently presented in some cases and there is no systemic approach to ensuring notices are always presented.	The organisation ensures that all Communication Forms include appropriate references and links to the Data Protection Notices.	The organisation maintains templates and regularly reviews all Communication Forms to ensure Data Protection Notices are embedded in forms with appropriate layering of content.	The organisation implements a formal change approval process to proactively ensure that Data Protection Notices are embedded in Communication Forms with appropriate layering of content.
Website (Cookies) and Forms The organisations website complies with transparency requirements and other relevant legislation ("EPrivacy") in the general website presentation and the use of cookies and other tracking technologies.	The organisation's website properties use cookies / other tracking technologies without gaining consent or providing notice to website visitors about the use of such technologies.	The organisation's website properties implement consent and transparency solutions which broadly comply with regulations.	The organisation's website properties implement consent and transparency solutions which fully comply with regulations and relevant guidelines and these are maintained.	The organisation regularly reviews its website properties for ongoing compliance with regulations and relevant guidelines.	The organisation proactively considers compliance with regulations and relevant guidelines when implementing changes to its website properties.

Category 4 - Legal Basis Management

The organisation identifies a reliable Legal Basis for each processing activity and ensures all processing activities are consistent with the identified Legal Basis.

1. LEGAL BASIS MANAGEMENT - OVERVIEW

The requirement to have a legal basis for processing personal data is central to compliant processing activities under the GDPR. Identifying a legal basis ensures that personal data is processed fairly and legally without adversely affecting data subjects. The GDPR provides a number of different legal basis which can be relied upon for processing, depending on whether the personal data being processed is general or "Special Category" personal data.

An organisation must record the legal basis for all its processing activities in the Record of Processing Activities ("ROPA") and may need to be able to provide evidence of what it presented to the data subject at the time it collected the personal data. For general personal data, the processing of personal data can be based on one of six legal basis specified in Article 6 GDPR, consent, contract, legal obligation, vital interest, public interest and legitimate interest. If processing Special Category personal data, the processing must be based on one of the six general legal basis identified above in addition to one of the legal basis specified in Article 9 GDPR.

Identifying and documenting the relevant legal basis in the ROPA is one of the first steps that many organisations take as part of their compliance with this category. This is quite an undertaking in and of itself. However, the real challenge is in meeting the requirements of the GDPR for the relevant legal basis. The validation work may, for example, include assessments around the vital interest, public interest or legitimate interest being pursued. These will need to be documented by the organisation and in some cases will need to be quite comprehensive.

Where consent/contract is being relied upon, the organisation will need to validate that it is clear from the information presented to the data subject that they were providing consent/entering a contract. If relying on legal obligation the organisation must be able to identify the particular piece of legislation that supports the processing activity. Additional validation will be required for the legal basis selected for any special category personal data.

2. LEGAL BASIS MANAGEMENT - GPDR ARTICLES

The relevant GDPR Legal Basis Management Articles are:

- **Article 5 (1)(a)** - Principles relating to the processing of personal data
- **Article 6** - Lawfulness of processing
- **Article 7** - Conditions for consent
- **Article 8** - Conditions applicable to child's consent in relation to information society services
- **Article 9** - Processing of special categories of personal data
- **Article 10** - Processing of personal data relating to criminal convictions and offences

3. LEGAL BASIS MANAGEMENT - CRITERIA

(a) Legal Basis Management Policies and Procedures

An organisation must have a clear and documented policy for managing its legal basis for processing personal data. This policy may be a standalone policy or incorporated as part of the Data Protection Policy of the organisation. Such a policy allows an organisation to demonstrate its GDPR compliance by clearly explaining the applicable legal basis under Article 6 and, where relevant, Article 9 GDPR.

The organisation should indicate which of the six general legal basis apply to the organisation's data processing. These are (i) Consent, (ii) Contract, (iii) Legal Obligation, (iv) Vital Interest, (v) Public Interest, and (vi) Legitimate Interest. Where special category personal data is being processed, in addition to the general legal basis, the organisation should identify the legal basis available under Article 9,namely: (i) Consent, (ii) Employment, Social Security and Social Protection Law, (iii) Vital Interests, (iv) Legitimate Activities of a foundation, association or not-for-Profit, (v) Manifestly made public, (vi) Exercise/Defence of legal claims, (vii) Substantial public interest, (vii) Preventative or occupational medicine, (ix) Public health, (x) Archiving purposes in the public interest, scientific or historical research or statistical purposes, and (xi) Member state legislation.

Some organisations may have a policy not to operate under a particular Legal Basis and this should be documented in the policy and communicated to staff.

Many organisations will have procedures around their marketing database and the management of their Legal Basis in certain circumstances. These procedures should be documented alongside the legal basis policy.

(b) Legal Basis Review

A valid legal basis must be identified for every processing activity undertaken in order to comply with the 'lawfulness, fairness and transparency' principle enshrined in the GDPR. Each organisation should undertake a review of its processing activities and ensure it identifies a valid legal basis for each activity. The legal basis should also be documented: this is usually done as part of the ROPA.

The legal basis must be communicated as appropriate to data subjects at relevant touch points. Particular care and attention will be required when communicating with data subjects if the organisation processes special category data, criminal offence data or biometric data.

(c) Legal Basis Assessments

There are certain assessments that should be documented by an organisation when relying on specific legal basis such as, public interest, vital interest and legitimate interest. Legitimate Interest in particular is usually assessed using a 3-part test known as a Legitimate Interest Assessment (LIA). As part of an LIA, an organisation must consider (i) if a legitimate interest is being pursued (ii) if the processing is necessary for the purpose and (iii) if the individual's interests override the legitimate interest of the organisation.

Working through this assessment process ensures that the organisation has clearly validated its legal basis and justified its rationale for relying on it. This is crucial because in the event a data subject objects to any processing undertaken, the burden of proof will be on the organisation to demonstrate the existence of a legitimate interest. Documented assessments may also be required by supervisory authorities in particular circumstances..

(d) Consent Management

Most organisations will be relying on consent for some processing activities. However, there are a number of challenges when processing on the basis of consent. In particular, the bar for meeting the compliance threshold for valid consent under the GDPR is high, and an organisation should maintain records demonstrating how and when that consent has been given. Appropriate structures need to be in place to ensure all aspects of consent are met including:

- the organisation must be able to demonstrate that consent was provided by the data subject
- consent must be clearly distinguishable and presented in clear and transparent language
- the data subject must be able to withdraw consent and withdrawal should be as easy as the provision of consent
- consent should be freely given

(e) Contract Management

Every organisation is likely to be processing some personal data on the legal basis of contract. An organisation must validate processing on this legal basis and ensure the personal data is necessary for the performance of the contract or in order to take steps at the request of the data subject prior to entering into the contract. Personal data that is not necessary for the performance of the contract will not be capable of being processed under this legal basis. For example, an organisation may want to process personal data for the purposes of biometric entry system into the workplace. It would not be able to use the contract of employment to support this processing as it is not necessary for the performance of the contract of employment.

4. LEGAL BASIS MANAGEMENT - FORT PRIVACY CASE STUDY

Client / Organisation: Credit Union

As part of our Data Protection Officer services for this Credit Union we documented a marketing policy to ensure that the lawful basis for processing was clear for all marketing activities.

Marketing in this context was undertaken by the Credit Union on the basis of legitimate interest.

We documented a legitimate interest assessment to ensure that the legitimate interest being pursued by the Credit Union does not outweigh the individual's right to privacy. This assessment did not happen overnight. A full checklist of activities were worked through over the course of a 12 month period to ensure that all compliance activities were in line.

The Marketing Policy was drafted to provide a clear approach for staff to use when undertaking any marketing activity to ensure that the legal basis can be relied upon in each case. We ensured that the ability to opt out was presented at initial touch points with members before any marketing was sent.

All systems and forms in the organisation were updated to ensure that the legitimate interest legal basis was supported. Relevant members of staff were trained to ensure a clear understanding of the approach.

In this case database management is really important. An unsubscribe is provided on each marketing communication and there are criteria that need to be followed to ensure that the content of the marketing communication is sent to the right members, e.g. it would not meet legitimate interest requirements to send marketing re loan services to a member in default.

5. LEGAL BASIS MANAGEMENT - MATURITY MODEL APPLICATION

Achieving the first levels of maturity in this category requires clear identification and validation of the legal basis for every processing activity in the organisation.

For organisations looking to progress to Level 4 or Level 5 maturity, the aim will be to reinforce each legal basis relied upon with supporting documentation. Legitimate Interest Assessments will need to be completed for certain processing activities. Maintenance and management of change in the organisation is really important as well as regular reviews of legal basis management activities.

The table below defines Level 1 to 5 for each Legal Basis Management Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Legal Basis Management Policies and Procedures The organisation's policies and procedures for legal basis management are fully documented, approved and implemented to ensure all processing activities have a documented Legal Basis.	Limited aspects of the organisations policies & procedures cover Legal Basis management or they only exist informally.	Policies and procedures addressing Legal Basis management exist and are fully documented.	Policies and procedures that address Legal Basis management are defined and implemented.	Compliance with policies and procedures that address Legal Basis management is measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with policies and procedures that address Legal Basis management are proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Legal Basis Review The organisation reviews and documents its Legal Basis for processing personal data. The legal basis is communicated to data subjects as appropriate.	The legal basis for processing is not fully documented for processing activities and communications with data subject is unclear.	Formal legal basis documentation and communication is undertaken. Legal basis may not be validated.	The organisation has documented, communicated and validated its legal basis in each case.	The effectiveness of legal basis identified is measured and reviews are conducted to assess the effectiveness of the validation activity undertaken.	Legal basis reviews are proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Legal Basis Assessments The organisation has identified all of its processing activities where assessments are required to validate the legal basis. If special category data is processed both an Article 6 and an Article 9 legal basis is identified and validated by the organisation.	Some assessments exist informally but may not be complete or fully documented.	Assessments exist and are fully documented.	Assessments and any resulting compliance activities are defined and implemented.	The effectiveness of assessments and their associated legal basis is measured and reviews are conducted to assess the effectiveness of the controls in place.	Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Consent Management The organisation has identified all of its processing activities where consent is the Legal Basis for processing personal data and has implemented appropriate notices and policies and procedures to ensure the organisation can rely on consent as the Legal Basis for the relevant processing activities.	Some consent management and related notices, policies and procedures exist informally but may not be complete or fully documented.	Consent management and related notices and policies and procedures exist and are fully documented.	Consent management and related notices and related policies and procedures are defined and implemented.	Compliance with notices and policies and procedures for consent based processing is measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with notices and policies and procedures for consent based processing is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Contract Management The organisation has identified and validated all of its processing activities where contract is the Legal Basis for processing personal data to ensure the organisation can rely on contract as the Legal Basis.	Some contract legal basis review and validation exists informally but may not be complete or fully documented.	Contract legal basis review, validation and communication is fully documented.	Contract legal basis review, validation and communication is fully implemented for all relevant processing activities.	The effectiveness of controls around contract legal basis activities is reviewed to assess the effectiveness of the controls in place.	The effectiveness of controls around contract legal basis activities is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.

Category 5 - Data Subjects Rights ("DSR") Management

The organisation implements policies and processes to facilitate and respond to data subjects who exercise their rights regarding the processing of their personal data.

1. DSR MANAGEMENT - OVERVIEW

Data protection is above all about the rights of data subjects. The main objective of data protection laws is to ensure the rights and freedoms of individuals are respected by those organisations that process their personal data.

Every data subject has rights that must be protected and which underlie the principles of data processing and the specific requirements for processing.

Since the GDPR came into effect some rights have been exercised more than others, in particular the right of access to personal data.

The GDPR outlines 9 fundamental data subject rights as follows:

1. **Right to be informed:** Data subjects have the right to be informed about the collection and use of their personal data.
2. **Right to access:** Data subjects have the right to view and request copies of their personal data.
3. **Right to rectification:** Data subjects have the right to request that inaccurate or outdated personal information be updated or corrected.
4. **Right to be forgotten/Right to erasure:** Data subjects have the right to request their personal data be deleted. Note that this is not an absolute right and may be subject to exemptions.
5. **Right to restrict processing:** Data subjects have the right to request the restriction or suppression of their personal data.
6. **Right to data portability:** Data subjects have the right to ask for their data to be provided to them or transferred to another controller. The data must be provided in a machine- readable electronic format.
7. **Right to object:** Data subjects have the right to object to the processing of their personal data.
8. **Right to object to automated processing:** Data subjects have the right to object to decisions being made with their data solely based on automated decision making or profiling.
9. **Right to withdraw consent:** Data subjects have the right to withdraw previously given consent to process their personal data.

It is important for organisations to inform data subjects about their rights under the GDPR. Implementing policies and procedure that set out the process for dealing with data subjects requests will help organisations manage these requests effectively and in a compliant manner. When organisations have these policies in place, they can be used to streamline the process effectively when data subjects invoke their rights, including setting out when a rights request should be refused, on the basis of the list of circumstances set out in Article 23 GDPR.

2. DSR MANAGEMENT - GDPR ARTICLES

The relevant GDPR DSR Articles are;

- **Article 7** - Right to withdraw consent
- **Article 12** - Transparent information, communication and modalities for the exercise of the rights of the data subject
- **Article 13** - Transparent information, communication and modalities for the exercise of the rights of the data subject
- **Article 14** - Information to be provided where personal data have not been obtained from the data subject
- **Article 15** - Right of access by the data subject
- **Article 16** - Right to rectification
- **Article 17** - Right to erasure (right to be forgotten)
- **Article 18** - Right to restriction of processing
- **Article 19** - Notification obligation regarding rectification or erasure of personal data or restriction of processing
- **Article 20** - Right to data portability
- **Article 21** - Right to object
- **Article 22** - Automated individual decision-making, including profiling
- **Article 23** - Restrictions

3. DSR MANAGEMENT-CRITERIA

(a) Data Subject Rights (DSR) Policies and Procedures

Organisations need to be aware of the rights of the data subjects whose personal data they are processing and the impact of such rights. An organisation needs to ensure that it implements policies and procedures for managing and responding to data subjects who invoke their rights. Organisations also need to review their communication and information materials (data protections statements) to ensure they set out the rights of the data subjects and their means for invoking those rights in a transparent way (see Transparency category).

(b) Data Subject Access Request

Article 15 GDPR gives individuals the right to request a copy of any of their personal data which are being 'processed' (i.e. used in any way) by 'controllers' as well as other relevant information. Data subjects are entitled to receive a copy of their personal data within one month and in most cases free of charge. Organisations should implement relevant policies and procedures outlining how to respond to and complete an access request within the required timeframe. Complying with these requests can be a burdensome task for some organisations however, implementing the right policies and procedures helps to streamline the process and facilitates the data protection team in complying with the request in a timely manner. The following are the steps for complying with a DSAR:

- Acknowledge receipt of the request and validating identity of data subject
- Gather all the personal data relating to the data subject into one location
- Review the gathered information for completeness
- Prepare the information for release by redacting any information that does not relate to the data subject or extracting information that does not need to be provided
- Release the information with a cover letter

(c) Right to rectification or erasure of personal data, restriction of processing and data portability

The GDPR provides individuals with the right to rectify their personal data. If a request is made the organisation will need to ensure that it updates or corrects inaccurate personal data. In many cases this can be very straight forward like an address change. There may be other more challenging circumstances where such requests are made and the organisation should have documented policies and procedures for dealing with such requests.

The GDPR provides individuals with the right to be forgotten/the right to restrict processing activities. This right may be exercised by individuals in varying circumstances. In some cases, an individual may not like information that has been published about them. In other cases, an individual may wish to be removed from a social media platform like Facebook or to restrict processing activities of an organisation. Organisations need to be able to respond to requests subject to the application of the restrictions set out in Article 23 GDPR.

The data subject has the right to request that their personal data be provided to them in a structured commonly used format for transmission to them or another provider under Article 20 GDPR. This right may be exercised where the processing is based on consent or contract and the processing is carried out by automated means. The controller should be able to facilitate transmission directly from one provider to another provider, e.g. from one mobile phone company to another.

(d) Right to object and automated individual decision making

Articles 21 and 22 of the GDPR cover the right to object and the right not to be subject to a decision based solely on automated processing. The right to object to processing is available for processing carried out on the legal basis of public interest or legitimate interest, including profiling undertaken on these grounds. If a right to object is received, the controller should no longer undertake the processing activity unless it is able to demonstrate compelling legitimate grounds for the processing that overrides the interests of the data subject. The legal basis assessments undertaken by the controller may be used to demonstrate this. The individual also has a right to object to any direct marketing: this is an absolute right.

Article 22 provides the data subject with the right not to be subject to a decision based solely on automated processing, which produces legal effects or otherwise affects the data subject. This right does not apply (i) if the decision is necessary for the performance of a contract or (ii) if the processing is authorised by law; or (iii) if the processing is based on express consent.

4. DATA SUBJECT RIGHTS MANAGEMENT - FORT PRIVACY CASE STUDY

Client / Organisation: Public Sector

We supported a client who received a significant number of data subject access requests at the same time creating a challenge to collate all the relevant data, redact it and release the information within the required timeframe. We provided practical guidance on structuring the information collected in order to effectively manage it through the review and release process including the use of redaction tools. We developed a review and redaction process to ensure the right level of information was released and the correct redaction procedures applied. We also reviewed all the released content giving the client confidence that it had met all its obligations in responding to the requests.

5. DATA SUBJECT RIGHTS MANAGEMENT - MATURITY MODEL APPLICATION

Achieving the first levels of maturity in this category requires clear policies and procedures for responding to rights that are likely to be exercised by data subjects in the relevant organisation.

For organisations looking to progress to Level 4 or Level 5 maturity, the aim will to be review procedures and identify areas where issues are arising when responding to requests and undertake relevant updates to address those issues.

The table below defines Level 1 to 5 for each DSR Management Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Data Subject Rights Management The organisation's Data Protection policies and procedures address mechanisms for the exercise of the rights of the data subject.	Informal Data Subject Rights policies and procedures exist.	Data Subject Rights provisions in policies and procedures exist and are fully documented.	Data Subject Rights provisions in policies and procedures are defined and implemented.	Data Subject Rights provisions in policies and procedures are measured and reviews are conducted to assess the effectiveness of the controls in place.	Management regularly monitors the processes and assignments of those responsible for policies and procedures relating to Data Subject Rights to determine their effectiveness.Where required, changes and improvements are made in a timely and effective fashion.
Data Subjects Access Requests A Data Subject is able to determine whether the organisation maintains Personal Data about them and, upon request, may obtain access to their Personal Data.	The organisation may have some informal procedures granting Data Subjects access to their personal data. Such procedures are not fully documented and may not be consistently applied.	Data Subject Rights provisions to allow Data Subjects to access their Personal Data exist and are fully documented.	Procedures to search for a Data Subject's Personal Data and to grant a Data Subject access to their information have been documented, implemented and cover all relevant aspects.Employees have been trained in how to respond to these requests, including recording such requests.	Procedures are in place to ensure Data Subjects receive timely communication of what information the organisation maintains about them and how they can obtain access. The organisation monitors information and access requests to ensure appropriate access to such Personal Data is provided.The organisation identifies and implements measures to improve the efficiency of its searches for a Data Subject's Personal Data.	The organisation reviews the processes used to handle Data Subject Access Requests to determine where improvements may be made and implements such improvements. Access to Personal Data is automated and self-service is provided when possible and appropriate.
Right to rectification/ erasure, restriction of processing and data portability Data Subjects are able to exercise these rights, upon request.	The organisation may have some informal procedures. Such procedures are not fully documented and may not be consistently applied.	Data Subject Rights provisions to allow Data Subjects to exercise these rights exist and are fully documented.	Procedures to enable these rights have been documented as applicable, implemented and cover all relevant aspects.Employees have been trained in how to respond to these requests, including recording such requests.	Procedures are in place to ensure Data Subjects receive timely communication and know how to exercise rights.The organisation monitors information and rights management.The organisation identifies and implements measures to improve the efficiency of its responses.	The organisation reviews the processes used to handle requests to determine where improvements may be made and implements such improvements. Where possible this is automated and self-service is provided when possible and appropriate.
Right to object and automated decision making Data Subjects are able to exercise the right to object and rights re automated decision making, upon request.	The organisation may have some informal procedures. Such procedures are not fully documented and may not be consistently applied.	Data Subject Rights provisions to allow Data Subjects to exercise the right to object/rights re automated decision making exist and are fully documented.	Procedures to enable rights to object/ rights re automated decision making have been documented as applicable, implemented and cover all relevant aspects.Employees have been trained in how to respond to these requests, including recording such requests.	Procedures are in place to ensure Data Subjects receive timely communication and know how to exercise rights.The organisation monitors information and rights management.The organisation identifies and implements measures to improve the efficiency of its responses.	The organisation reviews the processes used to handle requests to determine where improvements may be made and implements such improvements. Where possible this is automated and self-service is provided when possible and appropriate.

Category 6 - Data Transfer Management

The organisation implements policies and processes to facilitate and respond to Data Subjects who exercise their rights regarding the processing of their personal data.

1. DATA TRANSFER MANAGEMENT- OVERVIEW

In most cases, transfers occur when organisations outsource some of their processing activities to suppliers. The most common example is a cloud storage system or an IT service provider such as amazon cloud or Microsoft Azure. A central feature of compliance requirements and managing these transfers is to put in place an Article 28 GDPR compliant Data Processing Agreement (DPA) with the supplier.

Article 28 identifies specific provisions that need to be included in the DPA. The DPA is a legal contract covering various requirements that need to be fulfilled by the parties and in particular the supplier organisation. The DPA will usually form part of the commercial agreement between the parties.

The GDPR also requires due diligence to be undertaken on suppliers. Due diligence is where assurances are sought from the supplier that personal data will be safeguarded. Due Diligence needs to be undertaken when onboarding a new supplier and maintained with ongoing checks after the supplier is onboard.

If the supplier is outside the EEA then additional safeguards will be required. The GDPR includes particular requirements for the cross-border transfer of personal data, and in particular the transfer of personal data to "**third countries**" (under the GDPR this is any country outside the EEA). Personal data can only be transferred outside the EEA if 'an adequate level of protection' is in place (Article 45(1)).

Perhaps one of the most onerous of compliance categories, Data Transfer Management raises many challenges for organisations. A proactive approach is necessary: ensuring customer/suppliers transfer arrangements are logged and continuously reviewed is key to achieving any level of compliance. Many organisations will require dedicated resources to address the compliance requirements in this category.

2. DATA TRANSFER MANAGEMENT – GDPR ARTICLES

The relevant GDPR Data Transfer Management Articles are;

- **Article 13** - Transparent information, communication and modalities for the exercise of the rights of the data subject
- **Article 14** - Information to be provided where personal data have not been obtained from the data subject
- **Article 15** - Right of access by the data subject
- **Article 28** - Processor
- **Article 29** - Processing under the authority of the controller or processor
- **Article 30** - Records of processing activities
- **Article 32** - Security of processing
- **Article 42** - Certification
- **Article 44** - General principle for transfers
- **Article 45** - Transfers on the basis of an adequacy decision
- **Article 46** - Transfers subject to appropriate safeguards
- **Article 47** - Binding corporate rules
- **Article 48** - Transfers or disclosures not authorised by EU law
- **Article 49** - Derogations for specific situations
- **Article 50** - International cooperation for the protection of personal data

3. DATA TRANSFER MANAGEMENT – CRITERIA

(a) Data Transfer Policies and Procedures

There needs to be a clear and documented policy for how the organisation will manage transfers of personal data to ensure that a consistent approach is taken. The policy should cover, owners, approach, the organisation's policy for onboarding suppliers, requirements around Data Processing Agreements, International Transfers and Transfer Impact Assessments. A number of procedure documents are usually required to implement the policy.

(b) Supplier Due Diligence

Before an organisation decides to engage a supplier, it must conduct a due diligence assessment to ensure the supplier can meet its obligations under the GDPR.

In many cases an organisation will need to create a project plan for managing its suppliers which includes:

(i) making a log of all suppliers who are processors of personal data (this can usually be identified from the ROPA) or the finance system

(ii) identifying commercial agreements, data processing agreements and technical and organisational documents available/received

(iii) undertaking due diligence assessments (depending on the supplier, this may be sent to the supplier or completed by the customer (based on information available from the supplier))

(iv) reviewing assessments and identifying any risks or compliance tasks arising

(v) ongoing review of supplier for continued compliance

The most essential part of supplier due diligence is the review of technical and organisational measures ("**TOMs**"). The supplier must satisfy minimum security requirements as appropriate to the level of risk that applies to the processing activity being carried out.

(c) Data Processing Agreements

If an organisation engages processors, it must put in place a data processing agreement which complies with the prescriptive requirements set out in, Article 28 GDPR.

The DPA must include information about the:

(i) subject-matter of the processing
(ii) nature and purposes of the processing
(iii) types of personal data
(iv) categories of data subjects
(v) rights and duties of the controller

Article 28 (3), also requires that the DPA should include:

- a requirement to follow the instructions of the customer
- confidentiality undertakings
- technical and organisational measures of the supplier
- authorisation from the customer for the engagement of sub processors
- support from supplier for responding to data subject rights requests
- support from the supplier for DPIAs
- operational requirements around the retention and deletion of data
- requirements on the supplier to submit to audits
- requirement to inform of any instruction received that might infringe on the GDPR
- requirement to report any incidents arising

(d) Intra Company Data Processing Agreements

This is a form of Data Processing Agreement in an Intra Group context.

All of the requirements specified above must also be covered in the DPA between group companies to ensure compliance with Article 28 where a group company operates as a "supplier" to another group company. This is a common occurrence for example where payroll is processed by a group company on behalf of all the other companies in the group. All intra group transfers should be documented as part of the ROPA and these should be covered in the Intra Company DPA. This is usually drafted as a corporate document that is signed by the relevant group companies that are transferring personal data between them at group level.

(e) International Transfers (Transfers outside the EEA)

Organisations need to have clear insight into where their personal data is being stored and processed. If their personal data is being stored in the EEA then the personal data is protected by the safeguards in the GDPR. If a supplier is outside the EEA, additional measures are required to support the DPA. The form of "transfer mechanism" may vary from transfer to transfer as a number of options are available under the GDPR:

- An adequacy decision may exist for the country outside of the EU. The list of countries that have been provided with adequacy is here.
- Standard contractual clauses
- Binding corporate rules
- Approved codes of conduct
- A legally binding and enforceable instrument between public authorities or bodies
- Derogations for specific situations

The most common mechanism currently in use is Standard Contractual Clauses.

When personal data is being processed in a third country and where some concerns arise regarding the safety of personal data there is the additional requirement to carry out a Transfer Impact Assessment ("TIA"). A TIA is a risk assessment of laws and regulations of a third country and how they might impact a data subject's ability to exercise their rights under the GDPR.

One of the key points arising from the European Court of Justice in the Schrems II judgment is that when using Standard Contractual Clauses for transferring data, the underlying transfer must be assessed on a case-by-case basis to determine whether the personal data will be adequately protected (e.g., because of potential access by law enforcement or national security agencies). This means carrying out a TIA.

The basis for carrying out a TIA is that while SCCs bind both parties in relation to their processing of personal data, they do not bind anyone else, such as any third country authorities that obtain that personal data. This means that the data exporter must verify "on a case-by-case basis" what protections apply and if necessary implement supplemental measures.

4. DATA TRANSFER MANAGEMENT - FORT PRIVACY CASE STUDY

Client / Organisation:Public Company Supplier Due Diligence

We worked with a client to implement a supplier due diligence process as part of their overall outsourcing activities.

The organisation uses suppliers which process personal data to varying degrees, including no personal data, limited personal data and significant personal data including health data. As a result, the supplier due diligence activity needed to account for the different processing risks depending on the processing activity of each supplier.

As part of the process each proposed supplier is first screened to determine which category they fit into. Suppliers that process no personal data go through finance due diligence as normal as part of their onboarding. Suppliers that process minimal personal data are asked to supply a Master Agreement, Data Processing Agreement, Sub-processor list and documented TOMs. These suppliers go through a desk based due diligence which involves i) examining the provided documents to formally assess their compliance with GDPR Article 28 and ii) assessing the adequacy of their TOMs.

All other suppliers are provided with a due diligence questionnaire. They are requested to provide the Master Agreement, Data Processing Agreement, Sub-processor list and documented TOMs in addition to completing the due diligence questionnaire. The supplier is formally assessed on the basis of the responses provided and that assessment is documented.

In some cases, suppliers are unable to provide the required documents but the business may decide to proceed with the supplier nonetheless. In this case the business assesses the risk of proceeding, a senior manager must sign off on the assessment and the business will supply its own DPA and TOMS for the supplier to agree to. This exception is reserved for low risk situations – suppliers that process anything other than minimal personal data would normally fail due diligence if basic compliance documentation cannot be produced.

The final decision to engage with the supplier rests with the business. As a result of this process the business is able to make a fully informed decision about their engagement of the supplier. Depending on the circumstances the business may decide to proceed but with additional controls in place to monitor the supplier, decide to proceed with a different supplier or require the supplier to provide evidence that the shortcomings have been remedied (or will soon be remedied) before entering into the contract with the supplier.

5. DATA TRANSFER MANAGEMENT - MATURITY MODEL APPLICATION

To reach the optimised level of maturity for this category, organisations need to identify and assess all transfers of personal data – remembering that personal data doesn't always need to physically transfer for it to fall within the definition of processing under the GDPR.

A due exercise should be formally undertaken and documented for all suppliers and all relevant contractual documentation should be available including DPAs, transfer mechanisms and TIAs. The organisation should regularly review its transfer management activity to ensure that it is updated as changes occur in the organisation and in the customer/supplier's organisation.

The table below defines Level 1 to 5 for each Data Transfer Management Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Data Transfer Policies and Procedures The organisation's Data Transfer related policies and procedures are fully documented, approved and implemented.	Limited aspects of the organisations policies and procedures cover data transfer management requirements.	Data Transfer related policies and procedures exist and are fully documented.	Data Transfer related policies and procedures are defined and implemented.	Compliance with Data Transfer policies and procedures are measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with Data Transfer policies and procedures is monitored proactively to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Supplier Due Diligence Appropriate due diligence is undertaken by the organisation before any Personal Data is transferred outside the organisation to another supplier.	Procedures to undertake due diligence prior to transferring personal data are informal, inconsistent and incomplete.	Procedures are in place and fully documented to ensure that due diligence is undertaken prior to any data transfer being initiated.	Documented procedures exist and are consistently and uniformly applied to ensure that adequate due diligence is undertaken before personal data is transferred outside the organisation.	Reviews of the effectiveness of due diligence activities are periodically performed.	Compliance with due diligence activities is monitored proactively to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Data Processing Agreements Personal Data is disclosed only to processors who have agreements with the organisation to protect Personal Data in a manner consistent with the relevant aspects of the organisation's Data Protection Policies and data protection laws. (Article 28 GDPR)"	Data Processing Agreements are informal, incomplete and inconsistently applied.	All required provisions are included in Data Processing Agreements.	The organisation can demonstrate that all required agreements are in place.	Regular reviews are undertaken to ensure that all required data processing agreements are in place and maintained.	Compliance requirements and updates to Data Processing Agreement are monitored proactively to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
International Transfers (Transfers outside the EEA) The organisation has documented all international transfers of personal data and ensured adequate safeguards are in place to protect personal data transferred.	Procedures to ensure appropriate safeguards are taken prior to transferring personal data outside of the EEA are informal, inconsistent and incomplete.	Procedures are fully documented to ensure that appropriate safeguards are in place prior to transferring personal data outside of the EEA.	Documented procedures exist and are consistently and uniformly applied to ensure that appropriate safeguards are in place prior to transferring personal data outside of the EEA .	Reviews of the effectiveness of the safeguards in place are periodically performed.	Safeguards for international transfers are reviewed and maintained proactively. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Intra company Data Processing Agreements The organisation has documented (i) all transfers of personal data within its group of companies and (ii) the roles of the parties to the transfer to ensure adequate safeguards are in place to protect personal data transferred.	Procedures to ensure appropriate safeguards are taken prior to transferring personal data between group companies are informal, inconsistent and incomplete.	Procedures are fully documented to ensure that appropriate safeguards are in place prior to transferring personal data between group companies.	Documented procedures exist and are consistently and uniformly applied to ensure that appropriate safeguards are in place prior to transferring personal data between group companies.	Reviews of the effectiveness of the safeguards in place and the completeness of the Intra group DPA are periodically performed.	Intracompany DPAs are reviewed and maintained proactively. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.

Category 7 - Data Management

The organisation manages personal data processing activities to ensure consistency with the principles of purpose limitation, data minimisation, accuracy and storage limitation.

1. DATA MANAGEMENT - OVERVIEW AND DESCRIPTION

Data Management is all about the way that personal data is managed in the organisation to ensure consistency and compliance with the principles in Article 5 of the GDPR. This category requires organisations to ensure compliance requirements address purpose limitation, data minimisation, accuracy and storage limitation.

In practice data management is implemented across the entire organisation. It needs to be considered when processing operations are being designed (purpose limitation). It should be considered when the organisation is first collecting data from data subjects to ensure only the personal data that is necessary is collected (data minimisation). The organisation needs to consider how long it will need to keep personal data and how it will dispose of that personal data when it is no longer required (storage limitation). Finally, while the personal data is still in use the organisation must ensure that it remains fit for the purpose (accuracy).

Data Management is a very challenging category for most organisations because it has such a broad remit. A well-documented and maintained ROPA will form the cornerstone for validating adherence to the relevant principles. Checks will be required to ensure that processing is limited to the purpose identified especially when the processing activities are being introduced. A review mechanism should be implemented to ensure that only required personal data is collected.

Where personal data is going to be relied on over a period of time, triggers should be put in place to ensure data is checked for accuracy when a new processing event occurs that will rely on that data. A robust data retention policy must be documented and fully implemented to ensure personal data is not retained longer than required and is securely deleted.

Having well-thought-out data management processes in place will help an organisation ensure robust compliance with the data management principles.

2. DATA MANAGEMENT - GDPR ARTICLES

The relevant GDPR Data Management Articles are:

- **Article 5 (1) (b)** - Purpose limitation
- **Article 5 (1) (c)** - Data minimisation
- **Article 5 (1) (d)** - Accuracy
- **Article 5 (1) (e)** - Storage limitation

Note for the purposes of the Framework the Data Management Category covers the principles in Article 5(1) (b) – (e).

Article 5 (1) (a) – (Lawfulness, Fairness and Transparency) is covered under the categories "Transparency" and "Legal Basis Management" and the principle of "Integrity and Confidentiality" under Article 5(1)(f) is covered in the Security category. The Accountability principal has its own category.

3. DATA MANAGEMENT – CRITERIA

(a) Purpose Limitation

The controller determines the purpose and means of processing and the legal basis for this processing. Article 5(1)(b) states: "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation**')"

In practice, this means an organisation must:

- be clear from the outset why personal data is processed and the purpose for which it will be used;
- have a clearly documented purpose for each processing activity;
- comply with transparency obligations to inform individuals about the purposes of processing; and
- ensure that if personal data is used for any other purpose that is additional to or different from the originally specified purpose, the new use is fair, lawful and transparent.

(b) Data Minimisation

According to Article 5 (1) (c), personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation'). Organisations need to validate personal data collection and ensure that only the minimum personal data is collected for the relevant processing activity. A well-documented ROPA should be the source of validation, however processes should be in place to check that all personal data collected at initial touch points with the data subject are reviewed to ensure no additional or unnecessary personal data is being collected.

Organisations should also seek to establish a process whereby the personal data being stored by the organisation is reviewed periodically. This will flag any unnecessary collection or reuse of personal data which may cause an organisation to be in breach of GDPR.

(c) Accuracy

Accuracy is a requirement of Article 5 (1) (c) of the GDPR. Organisations must take necessary steps to ensure the accuracy of personal data collected from data subjects and that they keep that personal data up-to-date. Organisations should ensure that they have procedures in place to review and update information periodically to ensure the accuracy of the personal data they are processing, particularly if it is being held over a long period of time.

(d) Storage Limitation

Personal data should only be retained for as long as is necessary for the specified purpose and thereafter, when it is no longer required, it should be disposed of securely. Documented retention policies and schedules should be detailed with information about each processing activity (aligned with the ROPA) and its related retention period. A formal retention schedule, provides documented evidence that justifies data retention and disposal periods and provides clear guidance for staff around retention periods for personal data.

Identification of an appropriate retention period is generally based on two key factors: (i) the purpose for processing the personal data; and (ii) any regulatory or legal requirements for retaining it.

A compliant retention policy and schedule should include the following:

- the personal data covered in the policy
- the retention period and the legal basis for retaining it
- the disposal method when it is no longer required.

4. DATA MANAGEMENT - FORT PRIVACY CASE STUDY

Data Collection (Forms) Review - Financial services sector

We completed a comprehensive review of all the forms that were being used by a financial services supplier to collect personal data in the provision of a variety of services.

Applying the principle of data minimisation, we tested each piece of personal data collected to ensure that it was necessary for the provision of the service and that the organisation had considered how long it would be necessary to retain the data. We also looked at the likelihood that the personal data would become out of date during the period it was retained and what provisions the financial services provider had in place to identify out-of-date data, to ensure it would not use such data and to implement mechanisms to update the data where necessary.

The scope of Personal Data collected via the forms was cross-checked against the Record of Processing Activities.

As a result of the exercise, we identified a number of instances where personal data was being collected that was not relevant for the service delivery – collection was as a result of copying one form to create a new form for a new service. We also identified instances where the provider was relying on personal data that was not being kept up-to-date posing a risk for both the service provider and the data subject. A process was put in place to ensure that the out of date information would not be relied on and the service provider would take steps to enable the service user to update their personal data more easily.

5. DATA MANAGEMENT - MATURITY MODEL APPLICATION

To reach the optimised level of maturity for this category organisations need to ensure that all processing activities are documented and validated to check the principles of purposes limitation, accuracy, data minimisation and storage limitation are being applied in the organisation. Training of staff is really important to ensure an understanding of these GDPR principles.

The table below defines Level 1 to 5 for each Data Management Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Purpose Limitation The organisation has identified all of its purposes for processing personal data and has implemented appropriate policies and procedures to ensure processing to limited to specified purposes.	Some purpose limitation policies and procedures exists informally but may not be complete or fully documented.	Purpose limitation policies and procedures exist and are fully documented.	Purpose limitation policies and procedures are defined and implemented.	Compliance with purpose limitation policies and procedures is measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with purpose limitation policies and procedures is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Data Minimisation The organisation has applied the principle of data minimisation to its processing activities and has implemented appropriate procedures to ensure that only the personal data required for the relevant processing activity is processed.	Some data minimisation procedures may exist informally but may not be complete or documented.	Data Minimisation procedures exist and are fully documented.	Data Minimisation procedures are defined and implemented.	Data Minimisation procedures are measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with data minimistation procedures is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Accuracy The organisation has applied the principle of accuracy to its processing activities and has implemented appropriate procedures to ensure that personal data processed is accurate and up to date.	Some data accuracy procedures may exist informally but may not be complete or documented.	Data accuracy procedures exist and are fully documented.	Data Accuracy procedures are defined and implemented.	Data Accuracy procedures are measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with data accuracy procedures is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Storage Limitation/Data Retention The organisation has applied the principle of storage limitation to its processing activities and has implemented appropriate procedures to ensure that personal data processed is retained for no longer than is necessary for the purpose.	Some storage limitation procedures may exist informally but may not be complete or documented.	Storage limitation procedures exist and are fully documented.	Storage limitation procedures are defined and implemented.	Storage limitation procedures are measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with storage limitation procedures is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.

Category 8 - Breach Management

The organisation implements policies and procedures to appropriately manage and respond to personal data breaches.

1. DATA BREACH MANAGEMENT - OVERVIEW

A 'personal data breach' is defined in the GDPR as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

This is further defined in guidance by the Irish Data Protection Commissioner as "a security incident that negatively impacts the confidentiality, integrity, or availability of personal data, with the consequence that the controller is unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 GDPR."

The GDPR imposes mandatory breach reporting and sets strict time limits for notification of a data breach to the relevant supervisory authority.

- Organisations are required to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals.
- Organisations must do this within 72 hours of becoming aware of the breach.
- Where a breach is likely to result in a high risk to the affected individuals, organisations must also inform those individuals without undue delay.

In order to meet the strict requirements around handling data breaches, organisation must implement processes to ensure staff are able to recognise breaches and know how to report these promptly. Processes are required to ensure incidents are investigated appropriately and that mechanisms are in place to assess consistently the requirement to notify the supervisory authority or to communicate with impacted data subjects.

It is considered best practice to investigate all incidents even those determined to be "near misses" as these investigations can help to identify underlying processing issues which could result in a more serious breach occurring in the future. This approach helps the organisation to implement robust preventative measures as part of their breach management activity.

2. DATA BREACH MANAGEMENT - GPDR ARTICLES

The relevant GDPR Breach Management articles are:

- **Article 33 -** Notification of a personal data breach to the supervisory authority
- **Article 34 -** Communication of a personal data breach to the data subject

3. DATA BREACH MANAGEMENT - CRITERIA

(a) Breach Management Policies and Procedure

Failure to properly manage Data Breaches from the outset will only exacerbate the problems for controllers or processors down the line. Organisations will need to document breach management policies and procedures that include sufficient detail to ensure that the policy of the organisation is very clear.

(b) Breach Identifications

Timing is critical when it comes to breach management, so having the proper reporting structures in place to ensure the correct individuals are notified when an incident occurs is crucial for GDPR compliance. Supervisory authorities, such as the Data Protection Commission in Ireland, require that organisations notify them of an incident within 72 hours.

Staff should be trained on breach identification so there is a clear understanding of what might constitute a breach of personal data. Staff should be advised regularly of simple steps required to report an incident, whether using a reporting tool or email to a particular address.

(c) Breach Investigation

Once the incident has been reported, organisations will need to complete a thorough investigation ideally using a breach investigation template. This document is designed to support effective reporting, investigation, mitigation and conclusion of incidents that may or may not constitute a breach of personal data.   All relevant information should be sought and reviewed to ensure a clear understanding of what happened and why it happened.

(d) Breach Notification

Following initial investigations there may be a requirement for controller organisations to report the breach to their supervisory authority “unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons”. If an obligation to report is identified the relevant breach notification form or process of the relevant supervisory authority will need to be completed. The Irish form is here.

Controller organisations will also need to notify breaches to affected data subjects “when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons”. Any such communications must be clear and describe in plain language the nature of the personal data breach.

Processor organisations will not need to notify breaches to the regulator or to data subjects unless instructed by the controller organisation. Processor organisations will be under a legal (the GDPR) and contractual obligation to notify the controller of any incident in accordance with the provisions of the Data Processing Agreement. Processor organisations should consider procedures for ensuring such controller notifications are undertaken in an organised and professional manner to limit any damage to the commercial relationship with the customer.

(e) Breach Prevention

Breach prevention involves reviewing breaches or near misses in the organisation to identify issues with processing activities. Oftentimes it makes sense to appoint a breach management team in the organisation who work together to identify risks and mitigate the effects of breaches. Data Breaches can be stressful for organisations particularly where the right resources are not in place to manage them. Working through breaches and ensuring responsibilities are assigned for investigation and mitigation of breaches builds confidence that will stand to the organisation if a major breach occurs.

4. DATA BREACH MANAGEMENT - FORT PRIVACY CASE STUDY

CLIENT / ORGANISATION: Medium sized multinational

Fort Privacy worked on a project spanning a couple of months with a multinational organisation. The organisation was seeking to completely overhaul their breach management process.

By implementing the Fort Privacy Framework including creating proper reporting structures (“Governance”), we were able to assist the organisation to fundamentally change the attitude of its staff towards breaches. Providing specific training helped raise awareness among staff members in how to recognise a breach.

The reporting structures that were created ensured that the relevant stakeholders were involved at an early stage in the investigation process and as such the chance of an incident going unreported was decreased significantly. The senior management team regularly review incident trends and an escalation process was put in place to ensure they were aware of serious incidents as soon as they were identified.

The organisation subsequently experienced a serious breach when a key supplier had a cyber security incident. In this instance, the depth of experience built up in the organisation in managing data breaches meant that they were in a very strong position to handle this very serious data breach with minimal disruption. They met all the reporting requirements to multiple supervisory authorities including being able to turn around all requests for further information within very short timeframes.

The early and confident reaction limited the impact of the situation on the affected customers of the organisation, ensured that the organisation was able to proactively manage the situation with their customers, preventing any resulting reputational damage (the breach was in media reports). and ensuring a very quick restoration of service.

5. DATA BREACH MANAGEMENT - MATURITY MODEL APPLICATION

To reach a basic level of compliance maturity in this category, organisations should at a minimum provide training to staff to raise awareness around the topic as well as documenting and implementing a Breach Policy. To progress towards the higher levels of compliance maturity, regular training and awareness programmes should be implemented to ensure staff understand how to recognise and handle a Data Breach. Clear reporting structures should be in place, so key stakeholders are involved from an early stage, as well as an oversight process to keep senior management informed. In order to achieve full compliance maturity, organisations should have a means of ensuring that any weaknesses identified in the organisation's processes throughout the investigation are addressed to prevent future incidents.

The table below defines Level 1 to 5 for each Breach Management Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Personal Data Breach Management Policies and procedures The organisation defines and documents personal data breach policies and procedures to identify, assess, mitigate and report all personal data breach incidents and to avoid future occurrences.	Some breach policies and procedures exist but are incomplete and do not address all aspects of breach handling, identification, assessment, notification and prevention.	Breach policies and procedures to identify security incidents, to assess incidents, to notify breaches and address all aspects of breach prevention are defined and complete.	Policies and procedures to identify security incidents, to assess incidents, to notify breaches and address all aspects of breach prevention are implemented and adhered to.	The effectiveness of Breach policies and procedures is measured and reviews are conducted to quantitatively manage the effectiveness of the controls in place to identify breaches of personal data.	The implementation of breach policies and procedures is proactively managed to deliver deliberate process optimisation.
Breach Identification The organisation has policies and procedures in place to identify incidents that may result in a breach of personal data.	Some policies and procedures exist but are incomplete/not documented and do not address all aspects of breach identification.	Policies and procedures to identify security incidents are defined and complete.	Policies and procedures to identify security incidents are implemented and adhered to.	Security incidents reporting and investigation activity is measured and reviews are conducted to quantitatively measure the effectiveness of the reporting mechanisms.	The identification of security incidents is proactively managed to deliver deliberate process optimisation.
Breach Investigation The organisation has processes in place to investigate if identified incidents have resulted in a breach of personal data.	Some policies and processes exist but are incomplete/not fully documented and do not address all aspects of breach assessment.	Policies and procedures to assess incidents are defined and complete.	Policies and procedures to assess incidents are implemented and adhered to.	Incident assessment activity is measured and reviews are conducted to quantitatively manage the effectiveness of the controls in place.	The assessment of incidents is proactively managed to deliver deliberate process optimisation.
Breach Notification The organisation has processes in place to notify the supervisory authority and the impacted data subjects (where required) of breaches of personal data.	Some processes exist but are incomplete and/or not documented and do not address all aspects of breach notification.	Policies and procedures to notify breaches are defined and complete.	Policies and procedures to notify breach of personal data are implemented and adhered to.	Breach notification activity is measured and reviews are conducted to quantitatively manage the effectiveness of the controls in place.	The notification of personal data breaches is proactively managed to deliver deliberate process optimisation.
Breach Prevention The organisation has processes in place to prevent future incidents that may result in a breach of personal data.	Some processes exist but are incomplete/not documented and do not address all aspects of breach prevention.	Policies and procedures to address all aspects of breach prevention are defined and complete.	Policies and procedures to address all aspects of breach prevention are implemented and adhered to.	Incident prevention activity is measured and reviews are conducted to quantitatively manage the effectiveness of the controls in place.	Incident prevention is proactively managed to deliver deliberate process optimisation.

Category 9 -Security

The organisation implements technical and organisational measures to manage the security of personal data and of systems that it uses to process the personal data

1. SECURITY - OVERVIEW

It is not possible to achieve data protection compliance by only considering data security. Equally it is not possible to achieve data protection compliance without considering data security. Ensuring the security of the personal data that is processed by or on behalf of the organisation is a fundamental requirement.

Article 32 of the GDPR identifies the requirements for data security. Organisations need to take a risk-based approach to data security while taking into consideration all aspects of the processing activities (nature, scope, context and purposes) and put appropriate levels of security in place.

The GDPR does not provide specific requirements but Article 32 does specify four key areas that should be considered:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of Technical and Organisational Measures (TOMs) for ensuring the security of the processing.

The Fort Privacy Framework considers the organisation’s TOMs to be a core deliverable in the security category.

Article 24 “Responsibility of the controller” states: “the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

Article 28 requires that controllers must only use processors who can provide sufficient guarantees to implement appropriate TOMs and undertakes contractually to ensure the security of the data. This requires that security requirements must flow down the processing chain.

2. SECURITY - GPDR ARTICLES

The relevant GDPR Security articles are:

- **Article 5** - Principles relating to processing of personal data
- **Article 24** - Responsibility of the controller
- **Article 25** - Data protection by design and by default
- **Article 30** - Records of processing activities
- **Article 32** - Security of processing

3. SECURITY – CRITERIA

(a) Security Policies and Procedures

The organisation should document a high-level information security policy that outlines the objectives for information security and documents roles and responsibilities for addressing the security and continuity of the systems and/or services provided. The information security policy should be formally approved by management who should in turn ensure all personnel are aware of and follow the organisation's information security policy.

A mature organisation will conduct annual reviews of its information security policies taking into consideration violations, exceptions, past incidents, past tests/exercises, and known incidents affecting other (similar) providers in the sector.

(b) Technical and Organisational Measures (TOMs)

Implementing TOMs assists organisations in building a culture of data protection and data security awareness, and ongoing improvement.

The documentation of a set of TOMs goes towards the organisation's ability to demonstrate compliance. The TOMs is an overview of all the various measures in place across the organisation that are relevant to the processing of personal data. The process of documenting TOMs helps to identify gaps in the organisation's measures.

The TOMs document provides a useful framework for the organisation to build its supplier and data transfer due diligence processes. Organisations reporting data breaches are regularly asked to provide their TOMs in the course of investigations by Supervisory Authorities.

(c) Security of key software systems

Security in organisations can broadly be split into two main areas – the first is the security of the systems in use by the users and the second is the security of the underlying infrastructure. Organisations split their various security related policies and procedures into different documentation sets. However, in general, systems security policies are user facing and network security, which relates to the technical configuration of the underlying infrastructure (storage, transport, firewalls etc), is the domain of the organisation's security experts.

Software systems are configured for security – various security controls are put in place such as access controls, and/or password rules. These rules can be enforced by the system but also rely on users to observe them. Organisations implement rules on the use of mobile devices, the installation of software on the organisation's devices, and/or password management and communicate these rules to users in a series of information security policies.

(d) Security of Network Infrastructure

Network infrastructure is configured for and monitored by the organisation to ensure that the organisation's assets are protected against internal and external security threats. Where the organisation's assets are not directly controlled by the organisation – for instance cloud storage or computing infrastructure - the organisation will determine the appropriate configuration including security measures that must be implemented by the service providers.

The organisation should document its network security requirements, proactively assessing risks and ensuring the requirements impose appropriate levels of security controls to mitigate those risks.

4. SECURITY - FORT PRIVACY CASE STUDY

CLIENT / ORGANISATION: Public Sector Body

Fort Privacy helped to organise and document the TOMs for a large public sector body. This involved engaging with various teams within the organisation including the data protection team, HR, marketing, procurement, IT and operations.

The primary goal of the exercise was to ensure a comprehensive set of TOMs was in place and that the key teams across the organisation understood their respective roles in implementing data protection measures. The exercise to document the TOMs helped to raise general awareness across the organisation about data protection.

Once the TOMs were documented, the organisation wanted to ensure that they were embedded into their procurement process. Given that this was a public sector organisation a very structured procurement process was in place which facilitated identifying the key places where TOMs could be embedded. The organisation was able to embed TOMs requirements into its RFQs for suppliers as well as documenting required TOMs into its standard contracts.

As a result, all contracts entered into by the organisation impose a set of TOMs that are communicated to suppliers early in the procurement process and which suppliers are required to commit to implementing as a core aspect of their service delivery.

5. SECURITY - MATURITY MODEL APPLICATION

Organisations looking to achieve a minimum level of compliance maturity with respect to this category can do so by first undertaking a review of their current TOMs. By undertaking this review process, organisations have the opportunity to prioritise the gaps in their current processes which they wish to correct.

Full compliance maturity is accomplished by organisations completing a full in-depth examination. Gathering these measures enables organisations to develop a roadmap of the key deliverables for the year ahead. As well as implementing these changes throughout their own group, organisations that achieve the highest levels of compliance maturity are expected to embed these within their supplier contracts to ensure the same levels of accountability are applied to each of their suppliers.

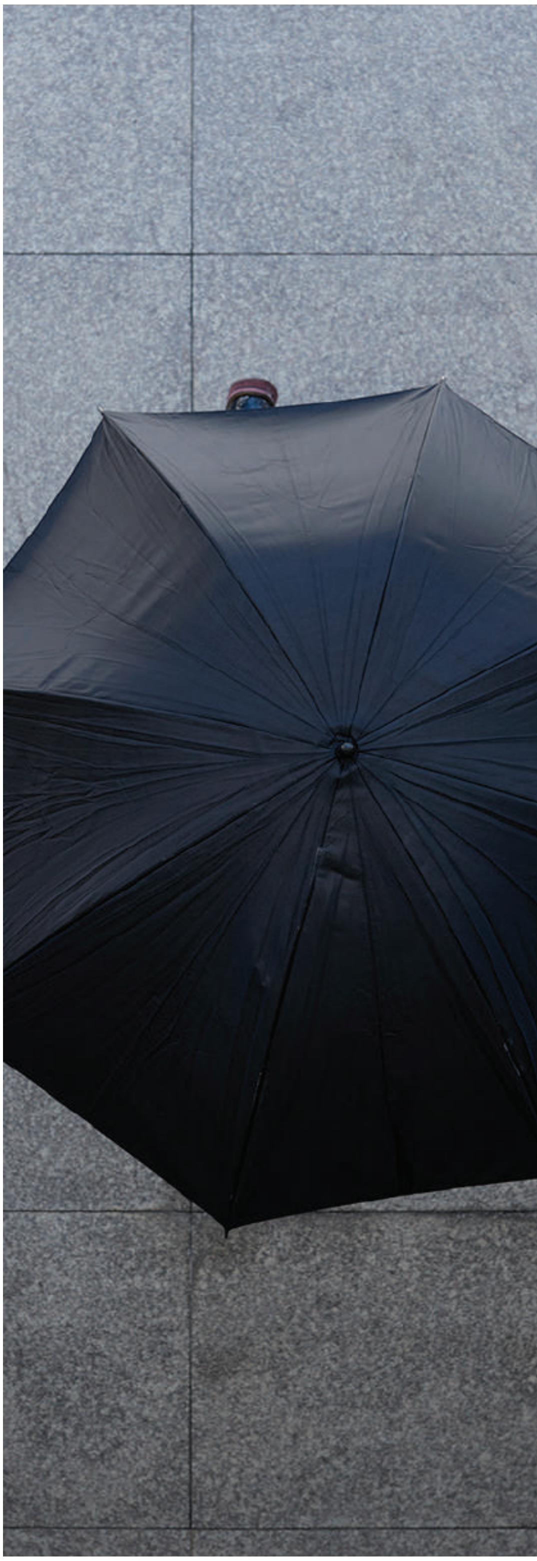
The table below defines Level 1 to 5 for each Security Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Security Policies & Procedures The organisation's Security Policies are fully documented, approved and implemented and ensure appropriate ongoing security for all personal data processing carried out by the organisation.	Limited aspects of the organisations Policies & Procedures cover the required security content or they only exist informally.	Security Policies and Procedures exist and are fully documented.	Security Policies and Procedures are defined and implemented.	Compliance with Security Policies and Procedures is measured and reviews are conducted to assess the effectiveness of the controls in place.	Compliance with Security Policies and Procedures is proactively managed to deliver deliberate process optimisation. Issues of non-compliance are identified, and remedial action taken to ensure compliance in a timely fashion.
Technical and Organisational Measures (TOMs) The organisation has implemented appropriate technical and organisational measures in order to demonstrate ongoing compliance with data protection laws.	Limited technical and organisational measures exist but these may not cover all areas and/or are not fully documented.	Technical and Organisational measures exist and are fully documented.	Technical and Organisational measures are defined and implemented.	The organisation conducts regular reviews to assess the effectiveness of its technical and organisational measures.	Technical and Organisational measures are regularly reviewed to relfect new guidance, judgements(ECJ) and legislative requirements.
Security of Software Systems The organisation has identified the key information (software) systems involved in the processing of personal data and has implemented appropriate procedures to ensure confidentiality and integrity of those systems.	Some information system security procedures exist informally but may not be complete or fully documented.	Information system security procedures exist and are fully documented.	Information system security procedures are defined and implemented.	The effectiveness of information security measures is measured. Systems are audited on a regular basis.	Information security measures are constantley revised and updated in line with best practices. Security capabilities of software systems is monitored and systems replaced if the security measures are no longer considered adequate.
Security of Network Infrastructure The organisation ensures the resilience of its network and ensures the ability to restore availability in a timely manner in the event of a physical or technical incident.	Some network security procedures exist informally but may not be complete or fully documented.	Network security procedures are fully documented and include back-up and restore and business continuity measures.	Network security processes are implemented.	The effectiveness of network security measures is proactively measured .	Network security measures are reviewed to ensure measures are updated to implement the current state of the art in response to network security risks.

Category 10 - Change Management

The organisation ensures that it manages changes to personal data processing activities to ensure ongoing compliance.

1. CHANGE MANGEMENT- OVERVIEW



Compliance is a journey and not a destination. The reality is that neither organisations nor compliance requirements stand still. The ability of any organisation to implement robust change management processes that consider compliance during planning, implementation and rollout of changes that involve the processing of personal data is key to ongoing compliance.

It is good practice to have policies and processes that ensure change is managed effectively. Those policies and processes should ensure that consideration is given to data protection risks and compliance activities as part of the change process. As a first step, the organisation will need to take steps to ensure that the DPO/DP Lead is consulted early in the process of planning new projects.

Article 25 of the GDPR places the onus on organisations to take a proactive approach to data protection when implementing change. Data Protection by Design may mean different things depending on the complexity of the organisation or the services or products that are under development. The underlying principle is a simple one however and involves embedding Data Protection considerations into the design process of new or updated products and services.

Article 35 of the GDPR requires a risk-based approach to change management. Organisations must consider whether the changes being introduced will introduce new risks to the fundamental rights and freedoms of individuals and take steps to mitigate those risks whenever possible. Where an organisation finds that it is not possible to mitigate those risks, Article 36 requires that the organisation formally consults with the supervisory authorities.

2. CHANGE MANAGEMENT-GDPR ARTICLES

- **Article 25 -** Data protection by design and by default
- **Article 35 -** Data Protection Impact Assessment
- **Article 36 -** Prior consultation
- **Article 39 -** Tasks of the data protection officer

3. CHANGE MANAGEMENT-CRITERIA

(a) Change Management Policies and Procedures

An organisation needs to develop policies and procedures around data protection requirements when implementing a new project in the organisation. The policy should outline the organisation's approach to managing change to ensure all key elements are addressed and effective processes and procedures are followed. It allows an organisation to systematically implement strategies to effect and control change and to provide support to employees to adjust to those changes. The policy will assign responsibility for monitoring compliance with the policy and to oversee the procedures when implementing changes.

(b) Data Protection Impact Assessment(s) – DPIA(s)

A DPIA is one of the key tools for managing compliance through the change process.

A DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". This is particularly relevant when a new data processing technology is being introduced. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still good practice and a useful tool to help organisations comply with data protection law.

DPIA Threshold Assessments assist organisations to determine whether the change in processing is considered "high risk" thereby triggering a legal requirement to undertake a full DPIA. Moreover, a good threshold assessment will provide a list of required compliance actions even where the threshold assessment determines that a DPIA is not considered necessary. There will nearly always be compliance updates to make as a result of a change. These generally include updates to ROPA, Data Protection Notices, DPAs, TOMs or policies and procedures. The organisation should record the threshold assessment to demonstrate compliance.

A DPIA is a risk and compliance assessment of processing operations. As part of any DPIA a review of the new processing activity should be carried out to assess the lawful processing of personal data and the level of appropriate TOMs in place, as required under the GDPR.

More specifically, Article 35 of the GDPR states that a DPIA should contain the following:

(a) a systematic description of the envisaged processing operations and the purpose(s) of the processing including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance considering the rights and legitimate interests of data subjects and other persons concerned.

(c) Data Protection by Design and Default

Data Protection by Design is primarily focused on how organisations will embed Data Protection compliance into their Change Management processes.

Data protection law allows organisations considerable flexibility in implementing Data Protection by Design programmes. However, such programmes must implement certain key elements, whatever the approach.

A Data Protection by Design programme should ensure that data protection impacts are considered throughout the entire project lifecycle. The organisation should undertake a risk- based approach –the DPIA Threshold Assessment and DPIA itself are key tools to be deployed as part of a Data Protection by Design approach.

Checklists are commonly deployed, and should ensure consideration of the rights of the data subjects, that the processing is lawful and that the processing is reviewed against the key GDPR principles. The project should also consider the effectiveness of measures that are implemented to mitigate risks or to ensure compliance. This means inclusion of KPIs or proactively considering how to carry out testing of new services for compliance.

Finally, there are design patterns that can be applied to product and service design to ensure that good data management practices are embedded.

4. CHANGE MANAGEMENT - FORT PRIVACY CASE STUDY

CLIENT / ORGANISATION: Industry Group

We undertook a DPIA on behalf of a user group for a software product. The user group consisted of a large number of data controllers who wished to deploy the product among their own customer base. As controllers they needed to ensure both that the product itself and their use of the product was compliant.

Because we carried out the DPIA on behalf of a large number of controllers we were able to engage very proactively with the processor during the product development and this enabled us to have a very positive impact on the design of the product itself. The engagement resulted in more focus on transparency within the user flow, which in turn provided a better user experience. The controllers benefitted from better uptake and from less queries coming through from product users.

Given that there were many controllers who would rely on the DPIA we ensured that the product was fully GDPR compliant if implemented out of the box and without changing any of the default configuration (data protection by default). We supplemented the DPIA with a guidance document so that controllers who wanted to change the default implementation could easily do so by adapting the DPIA to reflect their own implementation. We ensured that the DPIA itself was structured so that each controller could easily “make it theirs” by reviewing the risk mitigation activities.

The approach taken cost more in the initial completion of the DPIA as it needed to consider not just one single implementation but all possible variations. The development of additional guidance documents for controllers also required additional effort. However, the approach was very cost effective when costs were shared between the controllers. The participating controllers also benefitted from feedback received as multiple controllers undertook rollout of the product and raised new questions that resulted in updates being made to the DPIA.

5. CHANGE MANAGEMENT - MATURITY MODEL APPLICATION

To reach an optimised level of maturity with respect to this category, organisations should ensure they have appropriate structures in place to support staff in managing change. These structures should clearly outline to whom staff should refer their concerns that a change might result in a high risk to data subjects while encouraging staff to embrace privacy by design concepts.

Those organisations that do not reach the highest levels of maturity are often those who have failed to embed Data Protection compliance into their culture. Threshold Assessments should be conducted regularly to assist staff in assessing whether a new product or development may pose a risk to the “rights and freedoms of natural persons”. Mature organisations will have a system in place to log and file these DPIA’s so that any compliance requirements identified can be actioned.

The table below defines Level 1 to 5 for each Change Management Criteria.

CATEGORY CRITERIA	LEVEL 1 – AD HOC	LEVEL 2 – ESTABLISHED	LEVEL 3 – IMPLEMENTED	LEVEL 4 - MEASURED	LEVEL 5 - OPTIMISED
Change Management policies and procedures The organisations change management Policies and Procedures includes consideration of the impact of any changes to personal data processing activities. The organisation ensures that changes to personal data processing activities are managed and executed according to a formal change control processes that ensures compliance aspects of the proposed changes are addressed before the changes are implemented.	Change management policies and procedures are partially defined, do not take into account data protection aspects of change or they only exist informally.	Change management policies and procedures are documented and consider the impact of any changes to personal data processing activities, commit the organisation to involve the appropriate personnel and to evaluate and address data protection risks as appropriate.	Change management policies and procedures that take into account data protection aspects of change are defined and implemented.	The effectiveness of the organisation's change management policies and procedures in addressing data protection aspects of change are measured.	The organisation's change management Policies and Procedures are proactively managed to optimise their effectiveness at addressing data protection aspects of change.
Data Protection Impact Assessments The organisation undertakes Data Protection Impact Assessments prior to the implementation of a processing change that is likely to result in a high risk to the rights and freedoms of natural persons.	Data Protection Impact Assessments are undertaken inconsistently or informally and without documentation of the outcomes. The determination of whether a DPIA is necessary is not formally documented.	The end-to-end procedure for carrying out Data Protection Impact Assessments is fully documented.	Data Protection Impact Assessments are consistently undertaken by the organisation using formally documented templates, tools and processes.	The effectiveness of Data Protection Impact Assessments in minimising risk and ensuring ongoing compliance is regularly assessed.	Data Protection Impact Assessment templates and procedures are regularly reviewed and updated to ensure continual effectiveness of the process.
Data Protection by Design and by Default The organisation is committed to the effective implementation of the data protection principles and data subjects' rights and freedoms by design and by default.	The organisation may identify objectives to implement a Data Protection by Design approach to change but the scope of the approach is not clearly defined.	A Data Protection by Design approach is documented in change management policies.	Data Protection by Design is documented and supporting project tools such as checklists are embedded across the entire project lifecycle.	The effectiveness of the organisations implementation of data protection by design is proactively measured during and post-implementation.	The approach to data protection by design is continually reviewed and updated based on both internal review and external developments in best practice.

info@fortprivacy.ie
www.fortprivacy.ie

FORT PRIVACY
Getting Data Protection Right