NYMITY

From Privacy Project to Privacy Program

Leveraging GDPR Compliance Initiatives to Create One Accountable Privacy Program in Order to Comply with Multiple Laws

Teresa Troester-Falk
Chief Global Strategist
Nymity

Alexys Carlton
Director, Information Assurance & Privacy Otter Products & Blue Ocean Enterprises

Jennie Hargrove
Global Data Privacy Manager
HID Global

Michael Scuvée
Chief Data Protection Officer
Coca- Cola European Partners

Authors

Teresa Troester-Falk
Chief Global Strategist
at Nymity

Leading Nymity's global privacy strategy, Teresa is a thought-leader in the privacy industry and helps identify the future needs of privacy professionals by engaging with customers, privacy and data protection regulators, key policy groups/think tanks and other privacy thought leaders. Teresa leads some of Nymity's key accountability research initiatives and collaborates with other internal leaders to help innovate privacy accountability and compliance solutions and ensure organizational success.

Alexys Carlton, Director,
Information Assurance & Privacy
Otter Products & Blue Ocean
Enterprises

Alexys Carlton is the Director of Information Assurance and Privacy for Blue Ocean Enterprises and Otter Products. Alexys is a privacy technologist with professional and academic backgrounds in IT, information security, privacy, and data compliance. Alexys leads a global privacy program for Otter Products and advises the diverse Blue Ocean portfolio of companies. Alexys has experience embedding privacy and security into operations to ensure compliance with global data protection regulations.

Jennie Hargrove,
Global Data Privacy Manager
HID Global

As a privacy professional with over 11 years of experience, Jennie has a strong background in global data privacy regulations, information security, and compliance. Jennie is responsible for implementing HID's Global Data Protection Compliance Program as well as managing day to day privacy needs for all business units and departments across HID Global.

Michael Scuvée
Chief Data Protection Officer
Coca- Cola European Partners

Michael Scuvée is a Data Privacy compliance expert with 20 years' experience in consulting, market research, service and manufacturing industry sectors. Michael currently holds the position of Chief Data Protection Officer at Coca-Cola European Partners (CCEP).
CCEP operates across 13 European countries and is the world's largest independent Coca-Cola bottler by net sales. Michael leads the company's global Privacy Program as he did previously at Adient.

Table of Contents

Introduction

What does it mean to move from a GDPR privacy project to a privacy program?

The GDPR came into effect on May 25, 2018. Leading up to this date, many organisations had determined that it would be practical to approach the many requirements of the GDPR as a "project" with various workstreams. To that end, project managers were engaged to assist with the compliance obligations, timelines and milestones in line with a project management methodology and an "end date" of May 25, 2018. However, as is well known, May 25 was actually the ***start date***, after which organisations had to be able to demonstrate GDPR compliance on an ongoing basis.

After this deadline, Nymity began to see a theme emerging among our clients. Because of the GDPR's heavy operational lift and the numerous workstreams that had been implemented for the May 25 deadline, many privacy officers were thinking about how they might leverage all of the work that was done in preparation for the GDPR. They wanted to do this in order to demonstrate an ongoing capacity to comply with the GDPR as well as potentially address legal compliance requirements with other laws (including the forthcoming California Consumer Protection Act[1] and Brazil's General Data Protection Law [LGPD]). Also driving this desire for harmonization of their compliance efforts were the 700+ privacy and data protection laws and regulations around the World that they were already grappling with prior to the introduction of the GDPR.

Setting the Context: Accountability and Compliance Under the GDPR

What is accountability and compliance under the GDPR?

If there were already more than 700 privacy laws and regulations before the GDPR was passed, why was the GDPR such a heavy operational requirement for companies and what does it mean to demonstrate compliance under the GDPR?

The accountability principle in Article 5(2) of the GDPR requires organisations to demonstrate compliance with the principles of the GDPR (e.g. lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage or retention limitation, integrity and confidentiality and accountability). Article 24 sets out how organisations can do this by requiring the implementation of appropriate technical and organisational measures to ensure that organisations can demonstrate that the processing of personal data is performed in accordance with the GDPR.

[1] CCPA: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

LGPD: http://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156201-pl.html

Article 5 Principles Relating to Personal Data Processing	**Article 24** Responsibility of the Controller
The Controller shall be responsible for and be able to Demonstrate Compliance with paragraph 1 ('accountability').	Taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, 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.

There are three obligations stemming from these provisions:

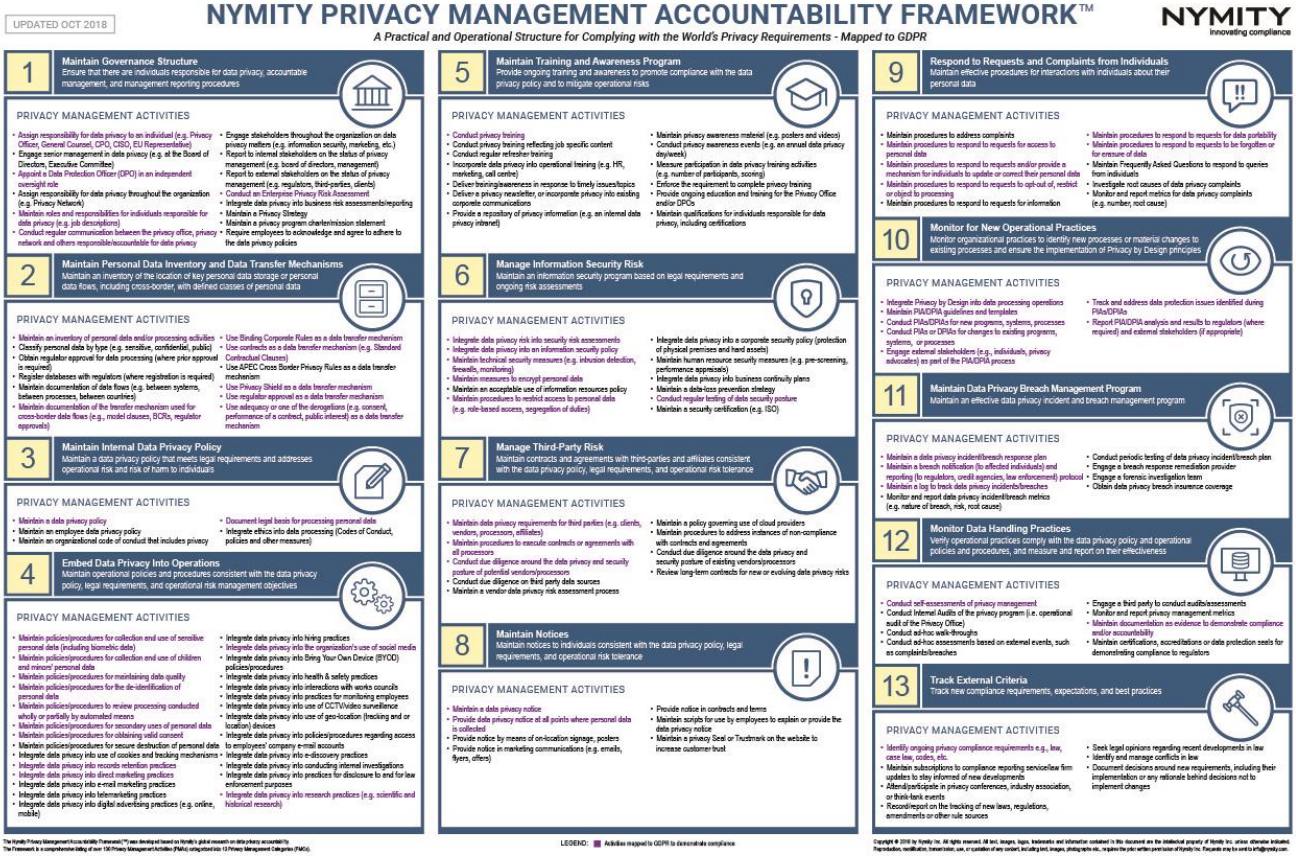
1. Organisations need to implement appropriate technical and organisational measures to meet the requirements of the GDPR;
2. Organisations need to ensure they can demonstrate their data processing operations are compliant with the GDPR;
3. Organisations need to ensure their technical and organisational measures are reviewed on a regular basis, and where needed, brought up-to-date.

Accountability (demonstrating compliance) means that at any time you need to be ready to explain *what* you are doing and *why* to all your stakeholders: business partners, individuals and most importantly the DPAs.

Regulators have made it clear that this is not a "tick-box exercise" but rather requires you to put in place a privacy program made up of appropriate technical and organisational measures in such away that you can maintain an ongoing capacity to comply. But what are those appropriate technical and organisation measures? The word is defined differently depending on the context, but in the context of privacy and data protection it is helpful to think about it as any kind of mechanism you put in place to mitigate privacy risk, for example, policies, procedures, guidelines, checklists, technology, training and awareness programs and technical safeguards.

Technical and organisational measures (privacy management activities) are any kind of mechanism you put in place to mitigate privacy risk, for example, policies, procedures, guidelines, checklists, technology, training and awareness programs and technical safeguards

Sample Privacy Management Framework for Operationalising and Demonstrating Compliance: A Menu of Technical and Organisational Measures



This image is a thumbnail view of the Nymity Privacy Management Accountability Framework™. It is not a "checklist" of requirements, but rather a "menu" of ongoing privacy management activities (technical and organisational measures).

In 2002, Nymity began our research on accountability and building compliance solutions for individuals responsible for privacy within organisations. In 2009 we enhanced this research through on-the-ground workshops around the World, including privacy and data protection regulators, examining what it would take for organisations to "demonstrate" accountability (e.g. internally to management or a board or externally to a regulator). Our research revealed that regardless of the industry or jurisdiction, privacy officers and other privacy leaders in organisations conduct many of the same activities. This led to the development of the Nymity Privacy Management Accountability Framework™ (the "Accountability Framework") which is a comprehensive list of 139 technical and organisational measures that is jurisdiction and industry neutral and structured into 13 data privacy management categories (for example "Manage Third Party Risk" and "Maintain Training and Awareness Program"). It has been made available to the global privacy community for free and has become a recognized framework used for a variety of purposes, including, structuring a privacy management program, baselining privacy

management programs, and for other research initiatives. The Accountability Framework also provides the privacy office with a structure to effectively define and communicate privacy management within its organisation and ultimately to demonstrate accountability. This Framework is kept up to date and modified appropriately, at least once a year. This framework maps to the OECD guidelines, all regulator guidance, the GDPR, the CCPA and over 700 other laws and regulations. The included Privacy Management Activities™ are not intended as a checklist, but instead form a menu of options to select from when developing a comprehensive privacy programme – by no means are organisations expected to implement all 139 activities.

Mapping the GDPR to the Framework

From the outset, Nymity's approach to GDPR compliance was to focus on the "end game:" the ability to "demonstrate compliance" which is found in Articles 5 and 24 of the GDPR. To determine what that would be, our expert Research Team mapped the Regulation to the Framework and identified 55 technical and organisational measures to be assessed, based on 39 articles of the GDPR (e.g. the appointment of a DPO, Records of processing, Data Protection Impact Assessments, Privacy by Design and Default, Data Subject Rights, Notices, Vendor Reviews etc.). It is the fact that 55 measures may be required to demonstrate compliance that made the GDPR such a large operational lift compared with all the laws that came before it.

To illustrate this further, the image bellow is a snapshot of Nymity's free GDPR Accountability Handbook (www.nymity.com /resources/GDPR Accountability handbook). The far-left column contains an operational summary of all 99 Articles of the GDPR, the next column identifies the appropriate technical or organisational measures followed by sample accountability mechanisms and specific examples of evidence that could be used to demonstrate compliance.

This table provides an overview of how a legal compliance obligation translates to practical and operational measures in your organisation.

Accountability Annotation	Technical or Organisational Measure	Example Accountability Mechanisms	Example Evidence	
Article 13 - Controllers obligations to provide notice to data subjects Article 13 provides that where personal data relating to data subjects are collected, controllers must provide certain minimum information to those data subjects through an information notice. It also sets out requirements for timing of the notice and identifies when exemptions may apply. See Recitals 60-62.	**Maintain a data privacy notice that details the organisation's personal data handling practices** This privacy management activity ensures that controllers put in place policies and procedures to ensure that the required information is provided to data subjects when their information is collected. **Maintain policies/procedures for secondary uses of personal data** This privacy management activity addresses having policies and procedures that define how to handle situations when the organisation wishes to use personal data beyond the primary purpose. Secondary uses of data must be disclosed in information notices under Article 13 and 14. **Provide data privacy notice at all points where personal data is collected** This privacy management activity addresses how an organisation provides an opportunity for data subjects to review the organisations privacy notice at the point of data collection.		Data privacy notice Just in Time Data Privacy Notice Mobile Data Privacy Notice Short Form/Condensed Data Privacy Notice Translated Data Privacy Notice Privacy Notice Language for Hard Copy Forms Privacy Notice Signage Privacy Notice in Marketing Communications Privacy Notice in Contracts and Terms Scripts for Providing Notice via Phone	Copy of the information notice provided to data subjects Documentation showing that privacy notice is aligned to legal requirements Details on the placement and timing of the notice Copies of contracts showing requirements for privacy notice language Records of training sessions with call center reps providing instruction on how to provide notice via phone

Evidence – Documentation is a By-Product of Accountability Mechanisms

Sample Project Approach to GDPR Compliance

Faced with the task of addressing up to 55 compliance requirements by May 25, 2018, many organisations enlisted support of project managers who approached the requirements with a traditional project management mindset as illustrated below in the following stages:

1. Assess the current program for GDPR readiness by identifying what already exists within the organisation for compliance
2. Identify where the gaps are (what already exists vs. what is left to be done)
3. Design specific solutions and remediation tasks required to address the gaps
4. Put in place the specific solutions and tools and conduct training an awareness campaigns to meet the end date of May 25, 2018.

Leveraging GDPR Initiatives to Comply with Other Laws

Organisations that invested heavily in a GDPR compliance project or infrastructure are now looking for opportunities to leverage those initiatives to both comply with additional laws and to create a sustainable privacy program. The below example illustrates how one GDPR compliance initiative (data subject access requests) may be used to address obligations in other laws.

Remediation Task: Maintain Procedures to Respond to Requests for Access to Personal Data	GDPR (Art.15)	CCPA	Brazil	Canada	Mexico	South Korea
	✓ 30 days (plus extensions)	✓ 45 days (plus extensions)	✓	✓	✓	✓
Leveraging GDPR compliance	Sample accountability mechanisms (remediation task solutions) that have been put in place to comply with GDPR Article 15 that may be used to comply with additional laws are: • Data subject access request form • Template letters for responding to requests • Subject access request log • Procedures for responding to customer requests and preferences • Customer service mailbox					

One Accountable Privacy Management Program may be Mapped to Many Laws and Regulations

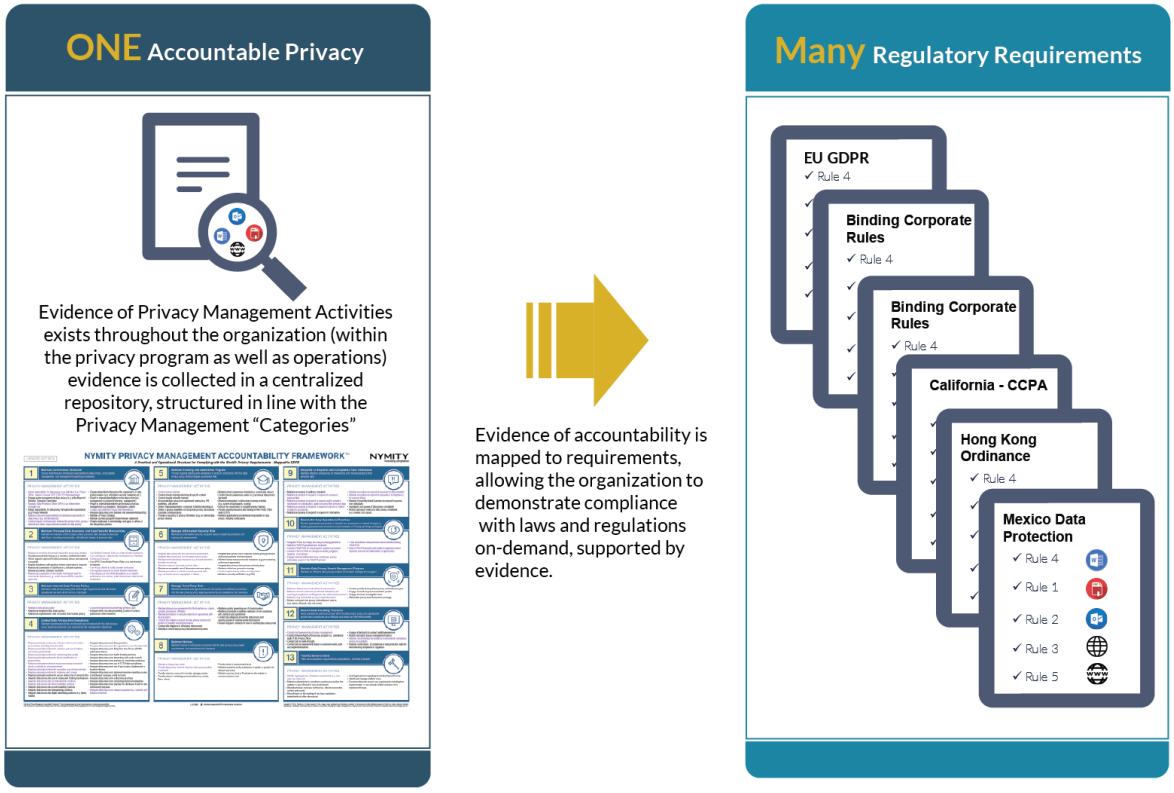
To create sustainable business processes going forward, rather than one-off law-specific project approaches (which involve work streams and remediation tasks) organisations are using the Nymity Privacy Management Accountability Framework™ to "find a home" for the deliverables of those workstreams in order to create a repeatable and scalable privacy program infrastructure and comply

with other laws, as required. This is privacy management accountability, which is a legal compliance obligation under the GDPR. Beyond the GDPR, the concept embodies what regulators expect of responsible organisations. Organisations that implement effective privacy management programs provide enhanced privacy protection, compared to organisations that take a purely compliance-based approach.

The images below illustrate how one accountable privacy program produces evidence that can be mapped to many regulatory requirements resulting in a repeatable, scalable and regulation agnostic privacy program.

Accountability	**Compliance**			
Privacy Management Categories	BCR	Brazil LGPD	EU GDPR	California CCPA
Maintain Governance Structure	✓	✓	✓	
Maintain Personal Data Inventory	✓	✓	✓	
Maintain Data Privacy Policy	✓	✓	✓	
Embed Data Privacy into Operations	✓	✓	✓	
Maintain Training and Awareness Program	✓		✓	✓
Manage Information Security Risk	✓	✓	✓	
Manage Third-Party Risk	✓	✓	✓	
Maintain Notices	✓	✓	✓	
Maintain Procedures for Inquiries and Complaints	✓	✓	✓	✓
Monitor for New Operational Practices	✓		✓	
Maintain a Data Privacy Breach Management Program			✓	
Monitor Data Handling Practices	✓		✓	
Track External Criteria	✓			

This results in one Accountable Privacy Program providing compliance with many regulatory requirements.



Conclusion and Next Steps

An accountable privacy program may produce evidence that can be mapped to many regulatory requirements resulting in a repeatable, scalable and regulation agnostic privacy program. Now that the theoretical overlap between multiple laws is clear, you can set to work to adapt your GDPR privacy project to deal with the many other laws that are relevant for your organisation.

1. To get started, first identify which privacy management activities that apply to GDPR as well as other relevant laws have been embedded in your organisation, and which policies and procedures you have implemented to ensure GDPR compliance. These policies and procedures are now up for review, and you will need to verify that all elements that are embedded in the other legal provisions are also part of your internal policies and procedures.

2. The next step is to take a look at the privacy management activities that are considered mandatory for other laws, but are not part of a standard GDPR compliance program. It may very well be that you have implemented these activities in your organisation. If so, you can repeat the check you have done described under step 1. If not, new policies and procedures are likely required. For job specific training program for example (a requirement under the CCPA) you could look to update the existing training program, and add a section on CCPA compliance. That would be especially relevant for your web editing, customer services and legal team.

To download Nymity free resources related to structured privacy management including the Nymity Privacy Management Framework ™, go to https://info.nymity.com/resources to learn more about how Nymity's privacy compliance software solutions can assist your organisation in managing your project level processes in a scalable and distributed manner, please see https://info.nymity.com/free-trial.

CASE STUDIES

Case Studies: From Privacy Project to Privacy Program

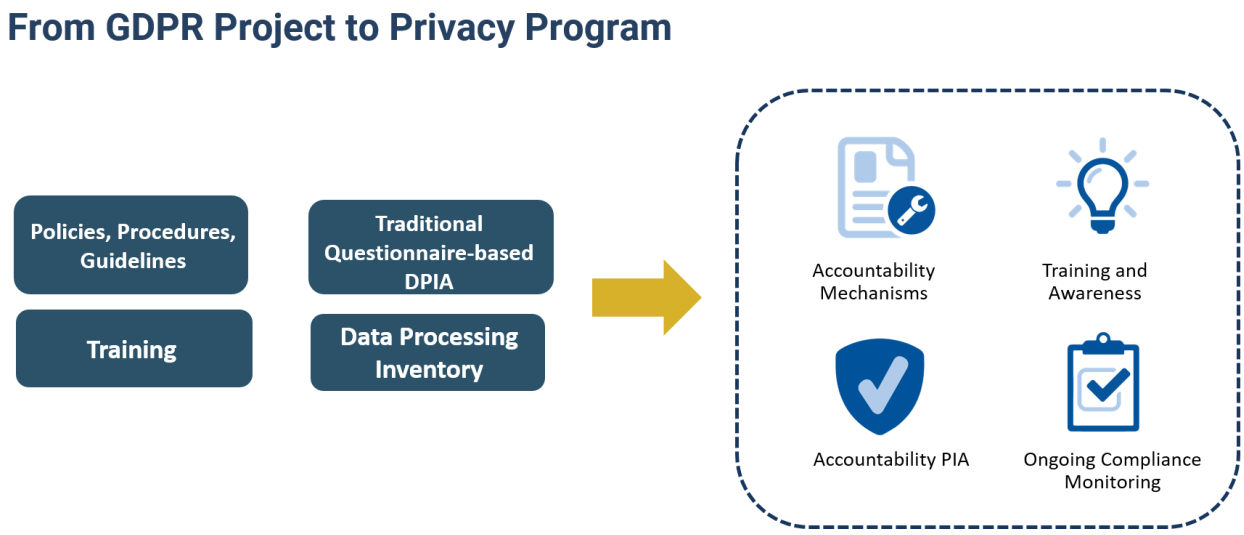
Case Study 1: From GDPR Project to Privacy Program

Jennie Hargrove
Global Data Privacy Manager
HID Global

As with most organisations doing business in the EU, the GDPR had prompted extra focus on data privacy at HID. Additionally, since the organisation was undergoing a transformation from a technology manufacturing company to a service provider, the Global Data Privacy Manager saw an opportunity to update how privacy had been traditionally managed at HID. The GDPR effort included conducting a privacy program gap assessment, developing a global data processing inventory, performing Data Protection Impact Assessments (DPIA) and executing remediation efforts around improving policies, procedures and guidelines to address GDPR and EU originating personal data. The result of these efforts was a privacy program to address GDPR for the May 25 deadline, but the program was heavily privacy-office focused and not yet global in scale.

At the time, the privacy office leveraged a traditional, questionnaire-based DPIA to complete risk assessments for processing activities involving personal data originating from the EU. This required training non-privacy personnel within the business on how to answer questions for the questionnaire-based PIA. The privacy office then reviewed each DPIA and made recommendations to the business.

Since the existing privacy office was small, the goal was to find a way to shift accountability to the business so the organisation could cover more risk and incorporate Privacy by Design (PbD) throughout the organisation. To that end, the Global Data Privacy Manager created a program consisting of accountability mechanisms, a new type of Privacy Impact Assessment (Accountability PIAs), training and awareness initiatives to empower the business, and ongoing compliance and monitoring of the program. The organisation had created a foundation of global policies and procedures that addressed regulatory requirements but now the goal was to develop procedures, work instructions and guidelines ***that could be leveraged more globally and in a more scalable, regulatory agnostic and efficient way for the organisation.*** To accomplish this, the organisation is taking the following steps:



Step 1: Assessment of Existing Accountability Mechanisms

The first step is performing an accountability mechanism gap assessment. HID had a great start using existing DPIAs which showed an inventory of privacy risk by function within the organisation. Using the existing DPIAs (which identified the privacy risk that was mitigated) along with the Nymity Privacy Management Accountability Framework ™, the privacy office is approaching business units and functions to conduct gap assessments against the existing processing activities and privacy risks. The goal is to create policies, procedures and guidelines that address both organisational privacy risk and regulatory requirements. The privacy office interprets the applicable privacy regulation for the business to ensure that the organisational accountability mechanisms address the requirements.

Step 2: Training and Awareness

After gap assessment and creating additional accountability mechanisms, the next step is conducting additional training and awareness campaigns to encourage the business to use the policies, procedures and guidelines. The training consists of a mix of computer-based training, PowerPoint presentations and periodic meetings with an extended privacy network within the business functions. The goal is to empower the business to appropriately handle typical data privacy issues they encounter and better incorporate privacy by design into their everyday job, regardless of the applicable regulations. This step provides the business with the instructions they need to follow in order to process personal data in the context of their job and helps shift accountability for mitigating privacy risk from solely on the privacy office to a shared responsibility within the organisation.

Step 3: Accountability PIA

The next step is shifting to an Accountability PIA methodology from a traditional, questionnaire-based PIA, where the business answers privacy related questions (which are at times, complex questions) and the privacy office reviews, looks for risk, makes recommendations and remediation plans. Rather than asking the business to answer questions and then making recommendations on steps to mitigate identified risk (which could be covered in an existing policy, procedure or guideline) the Accountability

PIA points to a relevant accountability mechanism and asks the business to attest to whether or not they have used the Accountability Mechanism for the processing activity they are recording in the PIA. When the PIAs are done, reports are generated which illustrate the risks that have been identified and the associated existing Privacy by Design (PbD) methods that demonstrate that the risk has been mitigated and how it has been mitigated. This reinforces to the business that there are existing guidelines that should be followed, rather than policies and procedures sitting in a repository that personnel are aware of but do not reference on a regular basis. By changing the dynamic of the traditional questionnaire-based PIA where the privacy office assesses risk and makes recommendations, Accountability PIAs reinforce the concept of PbD by encouraging the business to use existing guidance to incorporate privacy requirements from the beginning.

Step 4: Ongoing Compliance Monitoring

An important final step is to periodically review the effectiveness of the Accountability Mechanisms (AMs). Using the Framework, most of the common requirements across existing obligations are covered. But occasionally outliers come up that need to be accounted for and there may be risks identified during the PIA process that are not covered by existing AMs. Periodically the privacy office reviews existing policies, procedures and guidelines to determine if both the business risks associated with personal information processing and the regulatory requirements the organisation is subject to are adequately addressed. The outcome of this is adjusting the AMs, perhaps adjusting training and awareness, and discussing better ways to mitigate privacy risk during the periodic extended privacy network meetings in order to meet the needs of evolving privacy risk and regulatory requirements.

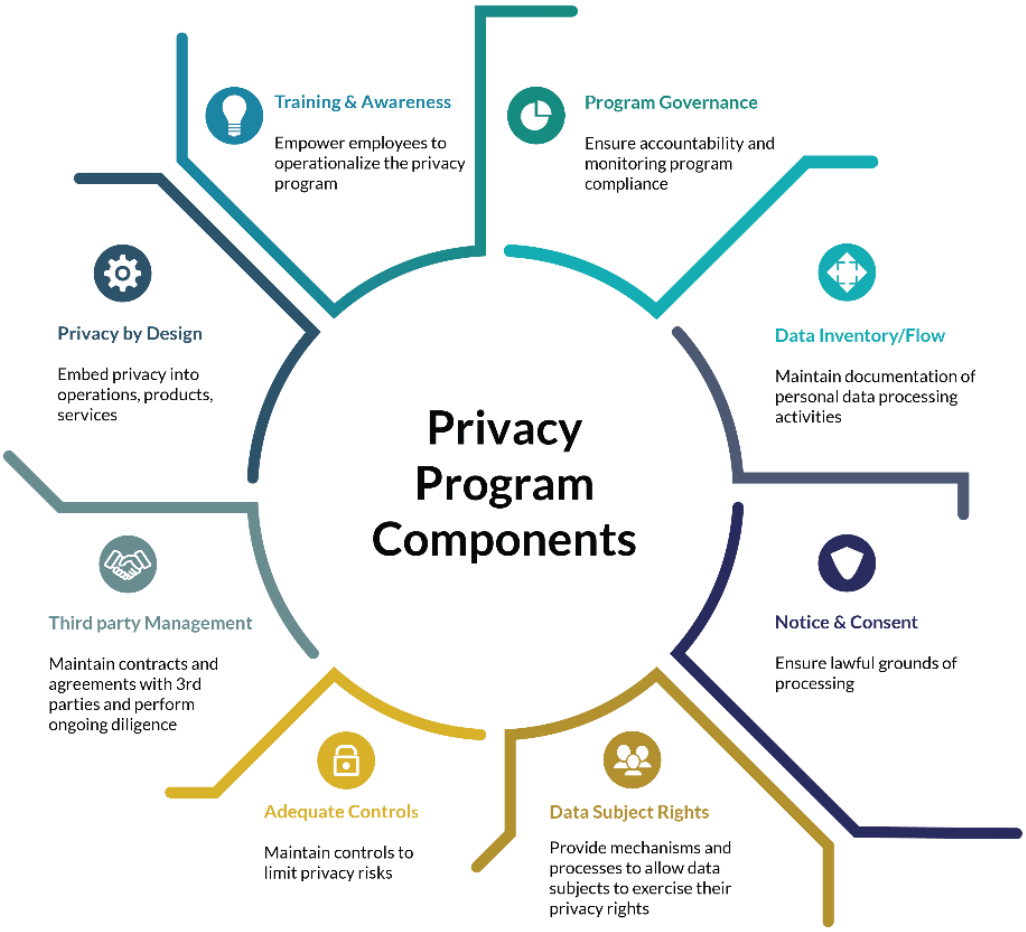
Case Study 2: A Framework Approach to Complying with Multiple Laws

Alexys Carleton

Director, Information Assurance & Privacy at Otter Products & Blue Ocean Enterprises

An ad hoc privacy management approach was not sustainable for a privacy office with one dedicated resource responsible for managing the privacy programs for a dozen diverse companies. The previous ad hoc privacy program was reactive to laws and regulations, and lacked a strategic focus to align to the business plan and to determine the appropriate privacy measures to implement to comply with multiple laws. The result was multiple privacy projects for each existing and new regulation and often a stressful time when responding to regulatory and business changes. This privacy director has implemented the Nymity Privacy Management Accountability Framework ™, including designing their GDPR readiness project based on the applicable technical and organisational measures that Nymity mapped to the regulation.

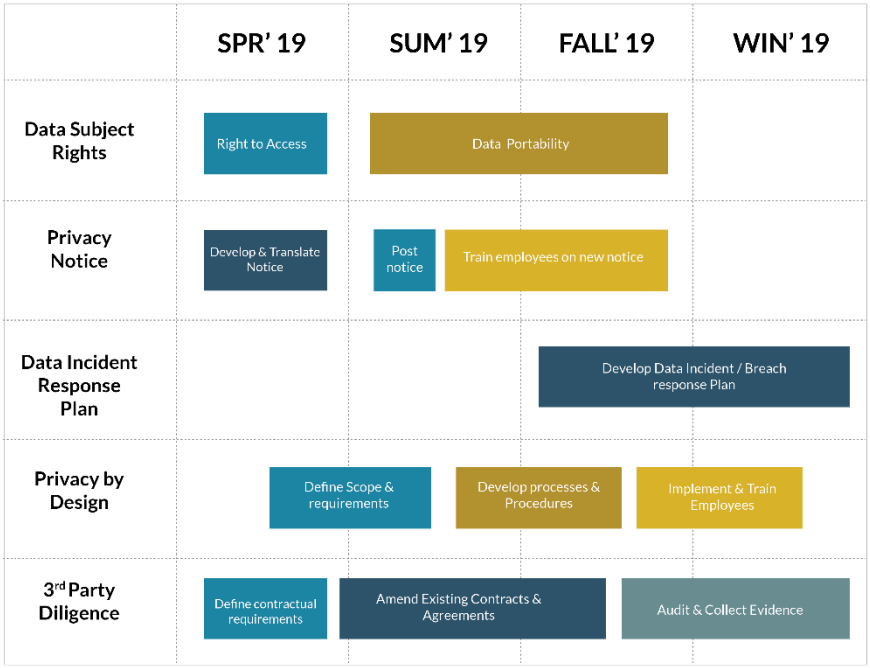
The Framework Implementation



Gaining leadership buy-in is critical to the success of any privacy program. The privacy director needed to not only communicate to leadership why a privacy program is important to the company but also the components that are required to make the program effective. The Privacy Director created a graphic entitled the *Resilient Privacy Program* to be used during conversations with other departments and company leadership to explain how the privacy office will operationalize the Nymity Privacy Management Accountability Framework ™. The *Resilient Privacy Program* represents the mature state of the privacy program and aids in the discussion about the technical and organisational measures that must be implemented to achieve this goal.

Following leadership buy-in, the Privacy Director worked cross-functionally to complete a gap assessment. The gap assessment defined the current state of the applicable Nymity technical and organisational measures and prioritised the activities the company would work to implement in the next year. The result was a privacy program roadmap which defined the projects necessary to remediate gap and operationalize each activity.

PRIVACY PROGRAM ROADMAP



Framework Utilization for a GDPR Project

New regulations or business operations can quickly change the focus of the privacy office and the applicable Nymity privacy activities. Shortly following the final announcement of GDPR, Nymity released the *GDPR Accountability Handbook* where they defined the 55 technical and organisational measures which mapped to GDPR. The Privacy Director performed a new gap assessment against these 55

technical and organisational measures and developed a GDPR readiness plan for each company comprised of many GDPR projects.

GDPR READINESS PLAN

The project deliverables were technical and organisational measures that prepared the companies to comply with GDPR but also helped to make the privacy program more mature and mapped to other global privacy regulations. The key was to design the measures in such ways that they can scale and map to multiple laws.

Using the Framework to Comply with Multiple Laws

Compliance requirements can absolutely drive the maturity of privacy program. However, implementing different measures for each privacy law would be an unsustainable privacy strategy for the multiple companies that this privacy director supports. If the compliance project deliverables align to the Nymity Privacy Management Accountability Framework ™, then over time these same measures can and should allow the company to be more resilient to change moving forward. In addition to 55 of the Nymity technical and organisation measures mapped to GDPR, 9 measures map to CCPA. As a result, this company has limited work to complete to prepare for CCPA. For instance, the data subject rights procedures already implemented measures for all individuals regardless of where they reside. These same measures can be utilized to honor the requests of EU or California residents.

The company has made an effort to embed privacy into operations through measures such as policies and procedures, guidelines, privacy impact assessments, and training. For instance, its data protection policies are global and jurisdiction agnostic. They moved away from using specific laws in its policies or

classifying data based on a legal requirement so that its employees do not have to think about the laws but rather what the company policy states. Mistakes and misinterpretations can easily happen if an employee has to identify and know the residency of the data subjects' personal data they are handling. Rather, the employees just need to know how to handle personal data.

Governing a Global Privacy Program

This company has made significant efforts to implement privacy measures in its organisations, especially preparing for GDPR. Measures put in place can be quickly be forgotten and employees often stop following policies and procedures. Every privacy program requires a governance structure to ensure the employees continue to follow processes, measures remain effective, and risks are being properly managed.

The Nymity Privacy Management Accountability Framework ™ includes information on maintaining a governance structure. For this company, governance goes beyond defining someone responsible for the program and gaining leadership support. It means transferring privacy accountability from the privacy team to the employees. It is an ongoing and focused effort. The governance program for this company consists of three main items: Accountability, Audit, and Assess.

Accountability refers to the implementation of policies, processes, procedures, and guidelines that ensure privacy is embedded into operations. The privacy professional cannot be in every meeting or oversee every task. Therefore, the department must empower employees to own the accountability measures that have been put in place.

Audit refers to putting some sort of function in place to check that the accountability measures the company has put in place are being followed and remain effective and appropriate for the business. This doesn't require a full internal audit. It can be separation of duties where employees keep each other accountability, or random spot checks. Additionally, audits give the privacy director the ability to obtain feedback and improve previous measures.

Assess refers to evaluating the effectiveness and maturity of the global privacy program. This company assesses the program at least once a year or upon any significant regulatory or company change.

Case Study 3: How to Integrate GDPR Project Components into a Sustainable, Operational Privacy Program

Michael Scuvée

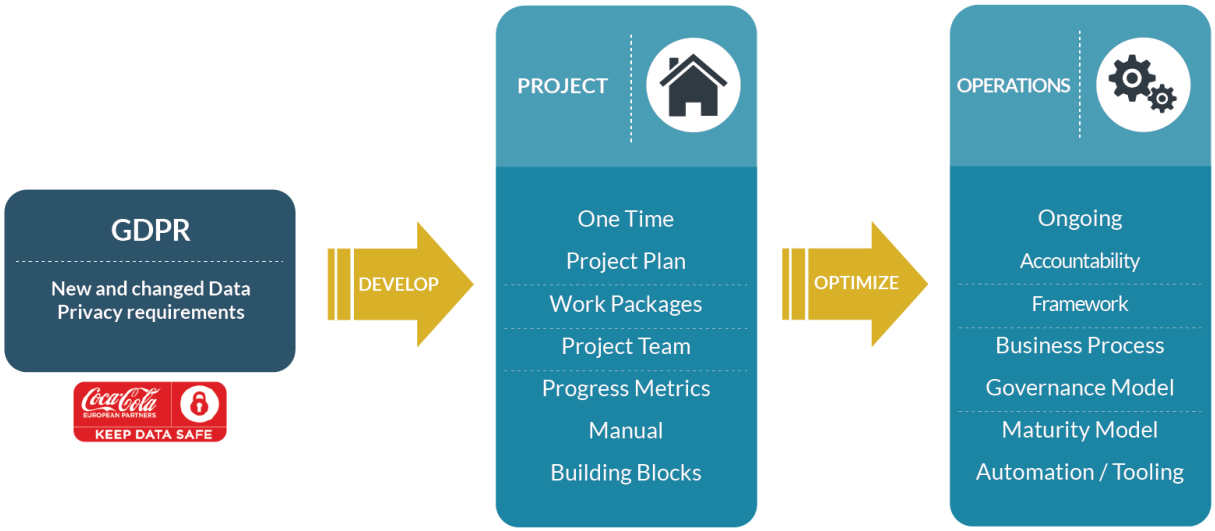
Chief Data Protection Officer, Legal Compliance,
Coca-Cola European Partners

The GDPR created a need for new controls or changes to existing controls for data privacy as there were so many different aspects that have been directly or indirectly affected by new requirements of the GDPR. The requirements spanned across many different compliance obligations including data subject access requests, Data Protection Impact Assessments (DPIAs), records of processing activities and other governance types of initiatives, Data Protection Officers and more.

A typical GDPR project started with a gap assessment and entering into a project mode centered on the deadline of May 25, 2018. The goal of such project mode is to get traction across the organisation and ensure timely delivery of the essential building blocks for GDPR compliance. Common project approaches have the end in mind. Typically, projects use the philosophy of a "one-time effort" and are organized around project plans, work packages and a project team approach (e.g. dedicated resources for the time of the project, steering committee oversight). The approach also generally includes progress metrics and tracking against a set deadline.

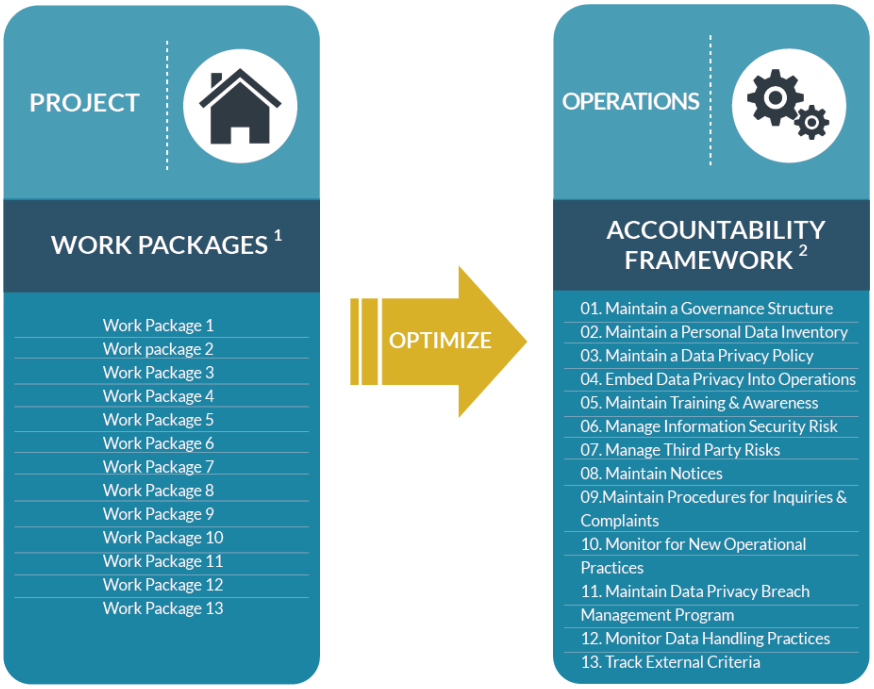
1. From One-time Project to Sustainable Business Operations

Importantly, the deadline of May 25 is the start of the journey, not the end. What is really important to understand is how all those project deliverables will find a home within an operational framework. After having put in place the GDPR compliance building blocks, organisations have to move from a project approach to ongoing processes where the newly created controls align to an accountability framework and translate into sustainable business processes. It is important to identify new functional stakeholders that need to integrate the operational Data Privacy Governance organisation as opposed to temporarily assigned functional project resources. This means embedding new or changed Data Privacy processes and controls within the organisation.



Instead of focusing on progress metrics, the focus moves towards adopting an accountability frameork, continuously measuring the maturity of the program and being able to benchmark against industry peers. To that end, automation and tooling play a critical role in making processes more scalable and sustainable.

2. From Project Work Packages to an Accountability Framework



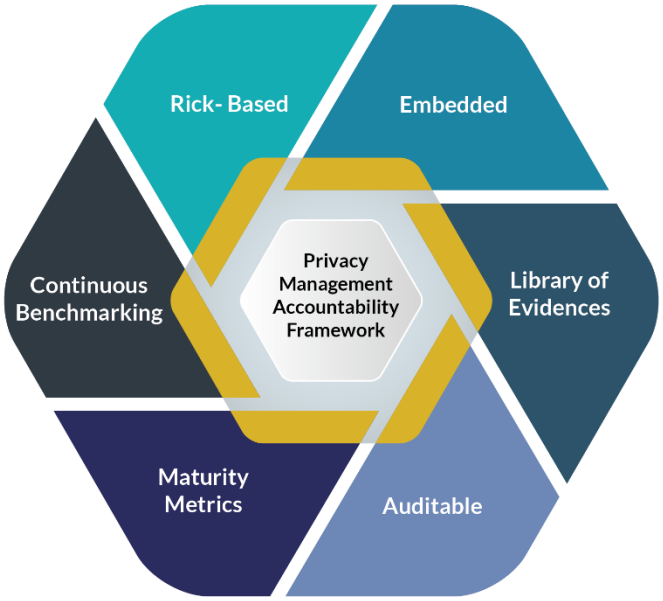
1. GDPR PROGRAM | 2. Nymity Privacy Management Accountability Framework™

In practice, many companies organized their GDPR project into work packages in order to implement the requirements (whether it is in strategy, assigning responsibilities for the new controls, creating records of processing activities or revisiting notices, policies and procedures). Those new controls need a new home in a stable accountability framework. The adoption of the Nymity Privacy Management Accountability Framework ™ makes it easy to identify a stable and natural home for the controls resulting from work packages and deliverables of a GDPR project

3. Demonstrate Accountability on Demand

At the end of the day, the name of the game is demonstrating accountability on demand. The GDPR requires organisations to be ready to demonstrate compliance to supervisory authorities at any time. Working and aligning GDPR controls within a stable accountability program helps you articulate your program and demonstrate it is risk-based and embedded within the operations of the company. It helps you organize a library of evidence which otherwise might be distributed across the organisation. Being able to provide the evidence of your program is critical, especially if you want to make your program auditable and transparent. The use of a commonly used industry standard framework also helps you conduct continuous benchmarking.

Data Privacy management tools can help you manage processes in a scalable and distributed manner. The interaction with business functions is essential to the success of a Data Privacy program. Therefore, business partners need to have a user-friendly experience when interacting with the privacy office. Technology can help provide such enhanced experience while enabling privacy offices to keep the pulse on the organisation and easily monitor operational processes and report on the status of the Data Privacy program.



4. Integrate GDPR controls into Accountability Framework

- Articulate your program
- Benchmark
- Demonstrate Accountability

5. Tooling the program plays a critical role

- Integrated Operational Processes
- Scalable & Distributed
- Central Oversight
- Enhanced Customer

HEADQUARTERS

Nymity Inc.
360 Bay Street, 6th Floor
Toronto, Ontario, M5H 2V6
Canada

+1 647 260 6230
Monday - Friday: 8:00 - 5:00 (EDT)

STAY INFORMED

www.nymity.com

linkedin.com/company/nymity-inc

@nymity