



# 2018 PRIVACY COMPLIANCE SOFTWARE BUYER'S GUIDE



---

The Ultimate Guide to Buying Privacy Software

---

# 2018 PRIVACY COMPLIANCE SOFTWARE BUYER'S GUIDE

## The Ultimate Guide to Buying Privacy Software

In many ways complying with privacy laws is straightforward:

1. Understand the legal obligations;
2. Build a privacy program made up of policies, procedures and other appropriate accountability mechanisms; and when there is sufficient volume and complexity;
3. Implement automated privacy management software.

Where compliance gets complicated, software can help organizations that have:

1. Operations in multiple jurisdictions; and/or
2. A privacy program that goes beyond a simple privacy policy; and/or
3. High volumes of, or complex, privacy management activities (e.g. Privacy Impact or Enterprise Assessments).

### About the Buyer's Guide

This Buyer's Guide helps a Privacy Office to navigate the different types of privacy compliance software and to best decide where to invest in order to mitigate risk, build accountability, and achieve ongoing compliance. The Buyer's Guide is focused specifically on software for the Privacy Office, but does not venture into other privacy-related solutions, including those covered in the IAPP 2017 Privacy Tech Vendor Report.<sup>1</sup> This Buyer's Guide has three objectives:

1. Help assess when software would be beneficial and provide a return on investment;
2. Provide example criteria for comparing different software solutions or when creating an RFP; and
3. Build a business case for the acquisition of required software solutions.

Also, the Buyer's Guide will address how software can help with ongoing compliance with the EU General Data Protection Regulation (GDPR) and how the GDPR could be part of the business case for software solutions.



*"The main driver behind the rapid growth in privacy technology appears to be Europe's General Data Protection Regulation, which comes into force in May 2018 with strict requirements and major consequences for non-compliance, though other regulations, like HIPAA in the U.S., the EU's pending ePrivacy Regulation, Canada's anti-spam law CASL, and cybersecurity laws in China and Russia, will continue to drive the market."*

IAPP 2017 Privacy Tech Vendor Report

<sup>1</sup> <https://iapp.org/resources/article/2017-privacy-tech-vendor-report/>

## Software for the Privacy Office

Since the first privacy laws, many organizations have assigned one or multiple individuals to maintain compliance with privacy laws, often called the Privacy Office or a Data Protection Officer (DPO). They need:

### Legal Research Software

Understand the ever-changing privacy compliance obligations and expectations around the world.

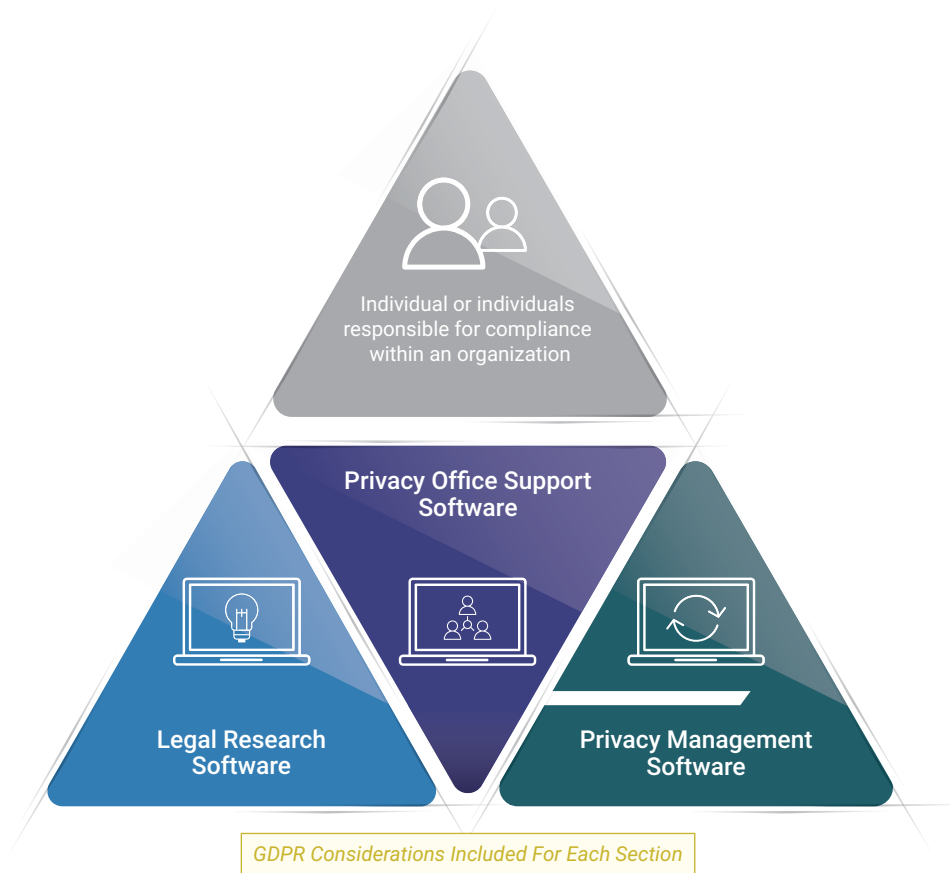
### Privacy Office Support Software

Build/maintain a demonstrably compliant privacy program that results in ongoing compliance.

### Privacy Management Software

Automate privacy management activities justified by volumes or complexity.

This Buyer's Guide investigates each of these three areas to help you decide if software will help you and your organization.



## What's the difference between Privacy Office Support Software and Privacy Management Software?

One of the key differences between support software for the Privacy Office and Privacy Management Software is that Privacy Office Support Software is used solely for the Privacy Office to support privacy compliance, while Privacy Management Software engages multiple responsible stakeholders throughout the organization.

Privacy Management Software, usually in the form of risk assessments, questionnaires, and expert systems, has been around for many years, while Privacy Office Support Software is reasonably new. Prior to Privacy Office Support Software, the Privacy Office had to rely on search engines, email, spreadsheets, and other forms of standard automation tools that were not specially designed for the Privacy Office.

# TABLE OF CONTENTS

## 01

### Legal Research Software

5-8

- *Understanding Compliance*
- *Reading the Laws*
- *The Business Case for Legal Research Software*

GDPR • *GDPR Considerations for Legal Research Software*

## 02

### Privacy Office Support Software

9-14

- *Build/Maintain a Privacy Program*
- *The Business Case for Templating Software*

GDPR • *GDPR Considerations for Templating Software*

- *Plan, Build and Embed Privacy Management Across the Organization*
- *The Business Case for Planning Software*

GDPR • *GDPR Considerations for Planning Software*

- *Baseline, Compare and Maintain Compliance*
- *The Business Case for Benchmarking Software*

GDPR • *GDPR Considerations for Benchmarking Software*

## 03

### Privacy Management Software

15-24

- *Determine when Automation is Required*

GDPR • *GDPR Considerations for PIA/DPIA Software*

- *Visually Document Data Processing Activities*

GDPR • *GDPR Considerations for Data Mapping Software*

- *Monitor/Report ongoing Enterprise Assessments*

GDPR • *GDPR Considerations for Enterprise Assessment Software*

## 04

### Software Vendor Considerations

25

- *Attributes to Consider when Selecting a Software Vendor*

## 05

### About Nymity

26-27

- *About Nymity: Privacy Compliance Software, Powered by Expert Research*
- *Software Solutions to Empower the Privacy Office*

GDPR • *Nymity and the GDPR*



## Section 1: Legal Research Software

The first consideration for any Privacy Office is legal research software. There is legal research software for all domains of compliance, and in the privacy space there have been dedicated solutions available for over 15 years. Most Privacy Offices that have existed for more than a year have legal research software, as it is the fundamental support software for the Privacy Office.

Legal research software provides the Privacy Office with necessary information to understand their compliance obligations either on-demand, typically in the form of a searchable database, or proactively in the form of ongoing alerts, reports or some other form of push knowledge. The premise is simple: *“How can the Privacy Office advise on compliance without up-to-date knowledge and a good understanding of legal requirements?”*



*“Quite simply, the sheer complexity large and small organizations face in managing consumer data is driving the need for scalable, efficient, technological solutions.”*

IAPP 2017 Privacy Tech Vendor Report



**Understanding Compliance:** Understanding the ongoing compliance obligations and expectations is a challenge. Not just finding them, but making sure a misunderstanding doesn't result in unnecessary restrictions on the business. Guidelines that are published by regulators and other authorities can be quite instructive, but tend to be long and sometimes provide limited insight into their impact on the business.

Apart from keeping track of the numerous authority documents published each year, the Privacy Office also requires access to information published in the past, which will still contain relevant expectations and obligations.

A good software solution will provide both a quick executive summary analysis and a structured operational analysis of all authority documents that would impact compliance, including regulator decisions and guidelines, court documents, new laws, bills, changes in law, etc.



**Reading the Laws:** Sometimes when reading a law, you need to track down detailed provisions for a specific business need, for example email marketing, data breach or cross-border transfers. Sometimes, you need details to help implement a specific privacy management activity, for example providing a notice or developing a policy.

Reading laws to find specific provisions that will impact a business operation is a challenge, especially for foreign jurisdictions, but a good software solution will enable laws to be quickly parsed to specific requirements, based on research already completed by experts in privacy laws. In some cases, a good software solution will enable a search-like function to identify requirements in law, and sometimes the requirements are provided at summary level in the form of a customizable chart or table.

**Staying Informed:** There are many free privacy news feeds and many law firms have communications about key developments in privacy compliance, but none cover all regulator decisions, regulator guidelines, court cases, bills or even changes to laws. To do so would require a large, dedicated research team. A good legal research software solution will cover all of the above, as such the software vendor would require a large dedicated privacy research team is in place.

**Informing Others:** The role of the Privacy Office is not only to stay informed, but also to inform others within the organization. A good legal research solution will enable the Privacy Office to easily keep others informed.

**Advising Stakeholders:** The Privacy Office is the location to which the business turns for privacy compliance advice. A good legal research software solution should keep the Privacy Office educated on key areas of privacy, but also be able to quickly provide them with the necessary information to respond to the business requests.

### **Legal Research Software = On-Demand & Push Knowledge**

Good legal research software delivers more than just time savings; it is a reduction in effort and increases in quality and accuracy; it also enables expertise on-demand. Good legal research software typically has two forms:

#### **1. On-Demand Knowledge**

Software that provides the ability to search and find specific information on the subject required. More advanced solutions will also provide both an executive summary and operational analysis related to compliance. In addition, good software will have the ability to provide pre-packaged research such as comprehensive comparative legal charts and maps.

When selecting a privacy research solution, it is important to evaluate the research division of the software vendor, to see if they employ proven privacy professionals dedicated to conduct the necessary ongoing research, and if they have a proven methodology for providing the analysis.

It is also important to see if they analyze the laws at a provisional level, not just provide a summary analysis. Summary analysis is important, but a good software solution will provide both summary and provisional breakdowns. They should also link regulator and court documents to the relevant provision(s) of law, to help ensure a quick lookup of compliance documents.

Lastly, at least for multinational organizations, all laws and analysis should be provided at least in English, even if the source document is in a different language.

### **RFP Considerations for Legal Research Software**

#### **Content Coverage**

1. Current – daily updates
2. Comprehensive – all jurisdictions
3. Historic – all relevant authority documents impacting privacy today
4. Provide executive summary in English
5. Provide operational analysis in English
6. Dedicated research team of privacy professionals
7. Analysis cross-linked to specific provisions in law
8. Cover laws, regulations, codes, guidelines, regulator papers, court cases, key bills, and other authority documents
9. Cover the over 700 global privacy-related laws (over 400 in the USA alone)

#### **Quick Reference Tools**

1. Up-to-date summary maps
2. Up-to-date comparative charts
3. Top development reports by specific subjects
4. Comprehensive breach support
5. Daily relevant alerts

#### **Thought Leadership**

1. Privacy Management Accountability Framework™
2. GDPR Compliance Materials
3. BCR and CBPR Compliance Materials
4. Demonstrating compliance support

#### **Expert Search Functions**

1. Business activities
2. Privacy principles
3. Jurisdictions
4. Specific laws and regulations
5. Type of legal document -for example, orders, opinions, litigation, guidelines
6. Legal keywords
7. Customer/employee privacy
8. Sources - courts, regulators, law firms
9. Industry
10. Date range

#### **Analysis Provided**

1. Executive analysis
2. Operational analysis
3. Risk/control analysis
4. Source document in original language

*cont'd*

## 2. Push Knowledge

Some privacy professionals rely heavily on push knowledge to stay informed in a timely manner. Push knowledge can come in the form of a daily relevant compliance alert, a monthly report, or an updated chart/map should there be a legislative change.

A good software solution will allow for push knowledge to be customizable to each individual that is receiving the information. The customization should enable that all relevant information is provided to each individual, while removing the information that has no bearing on compliance activities for that individual.

Push knowledge should come in a form that can easily be used by the individual to inform others. This will likely require special licensing considerations. Review the terms and conditions carefully to ensure the knowledge can be shared with others within the organization.

It's impossible to achieve compliance without understanding the compliance obligations. Without compliance knowledge, the risks are high that processing of personal data will be overly restricted and put unnecessary limitations on the business, or the necessary means for processing personal data in a legal manner will not be implemented.

### RFP Considerations for Legal Research Software

#### Alerting Service

1. Comprehensive – all jurisdictions
2. Customizable – select jurisdictions
3. Structured summary analysis to enable quick knowledge transfer
4. PDF generation and forwarding content
5. On-demand report generator for a specific purpose
6. Expert filters for automated report creation

#### Reporting

1. Multiple preconfigured popular reports
2. Customizable reports
3. Reports provided in MS Word for ease of editing and use as management reports or newsletters
4. Staying current reports
5. Trending reports

#### Quality Control

1. QA process for all published content
2. Update older content when relevant
3. Cross-link relevant and historical content

#### Support

1. Provided by privacy professionals
2. Online chat
3. Email/phone support
4. Training any time

## The Business Case for Legal Research Software



### Compliance

How can you be compliant without understanding your legal obligations and regulatory expectations? For both existing and new data processing operations, the software will support discovery of legal obligations and regulatory expectations, including when obligations and/or expectations change. This allows the Privacy Office to inform the business of any operational changes required to continue to ensure compliance.



### Risk

Not only the risk of non-compliance should be borne in mind, but also the risk to individuals whose information is being processed, the risk of violating contracts with 3rd party processors, and the risk of data breaches need to be considered. There are many risks that a good legal research solution can help identify and mitigate.



### Accountability

Legal software can demonstrate that the Privacy Office is supporting the organization's accountability, that timely advice is being provided to the business, and that the Privacy Office contributes to updating policies and procedures. Software can demonstrate to management, auditors, and regulators how the Privacy Office is monitoring compliance obligations.

The bottom line is that a legal research solution is the cornerstone of most Privacy Offices' compliance programs, as it provides them with a solid foundation of knowledge.

When looking for compliance software for the Privacy Office, it is best to start with a legal research solution.

### GDPR Considerations for Legal Research Software

Although the GDPR was designed as a single law for all EU Member States, the legislator has left some margin of manoeuvre at the national level. This means that in addition to the GDPR, organizations will need to keep track of the national data protection laws supplementing the GDPR in Member States where they have operations, for example in order to assess the age of consent and data processing in the healthcare or education sector.

Due account should also be given to specific regulator guidance. Across the EU, 28 national data protection authorities (DPAs) will supervise the correct application of the law. In addition, Spain and Germany have regional DPAs, which take over some of the supervisory obligations in their territories. All these DPAs are empowered to provide guidance on the application of the GDPR and the additional national legislation, and to start investigations, inquiries and/or enforcement action in case of (suspected) non-compliance. EU-wide, the European Data Protection Board will continue the work of the Article 29 Working Party in providing general guidance on the application of the law, and writing opinions on many other privacy and data protection related matters. Finally, it is expected the new law will also quickly find its way to the courtrooms across the EU at a regional, national, and EU level. Although it may take some time before the first cases are decided, it is already certain that GDPR-related case law will influence the application of data protection laws across the world, as was the case in recent years under Directive 95/46/EC.

All in all, just for the GDPR, there is a lot of information forthcoming that the Privacy Office will need to monitor. Legal research software can ensure the Privacy Office is indeed able to maintain up-to-date knowledge on privacy and data protection related developments across the EU, even if limited time is available.

### Nymity's Legal Research Software Solutions include:



NYMITY  
**RESEARCH™**

The Definitive Source for Privacy Compliance Research



ASK ABOUT OUR  
GDPR ADD-ON



NYMITY  
**LAWTABLES™**

Cross-Jurisdictional Rules of Law On-Demand



ASK ABOUT OUR  
GDPR ADD-ON



NYMITY  
**MoFoNOTES®**

Expert Summary Analysis of Privacy Laws



ASK ABOUT OUR  
GDPR ADD-ON



## Section 2: Privacy Office Support Software

One of the key responsibilities of the Privacy Office is to build and maintain an effective privacy program. A privacy program consists of policies, procedures, and other accountability mechanisms. To do so the Privacy Office will often be comprised of individuals responsible, albeit not always dedicated, to privacy compliance.

This section of the Buyer's Guide looks at privacy software that supports the Privacy Office to:

1. Build/Maintain a structured Privacy Program
2. Manage a Privacy Office Team
3. Benchmark a Privacy Program internally and externally



### **No Shortcuts**

*There is only one way to achieve ongoing compliance: an effective privacy program. There are no shortcuts. Privacy programs are enabled by the implementation of policies, procedures, and other accountability mechanisms, sometimes referred to as governance.*

## Templating Software

### **Build/Maintain a Privacy Program**

How can software help a Privacy Office build and maintain an effective privacy program? As a privacy program is made up of policies, procedures, and other accountability mechanisms, a software solution that would allow the Privacy Office to build and maintain these mechanisms would be very helpful, if only to avoid reinventing the wheel. This type of software is typically called templating software, as most Privacy Offices would assume sample documents ("templates") should be available for their requirements. However, an online search for such templates often results in poor quality and/or government-related sample documents, that are not easy to re-use.

A good software solution for templating will provide multiple and up-to-date supporting documents to allow the Privacy Office to create what is required for their privacy program. Nymity's research has identified 248 unique privacy management accountability mechanisms which are broken down as follows: Agreements, Audit/Assessment/Assurance, Certification, Communication, Consent Forms/Records, Governance, Job Aids, Legal Document/Process, Monitoring/Reporting, Notice, Operational Document, Physical Infrastructure, Policy, Procedures, Process, Records, System, Technical Configuration, Tools, and Training.

### **RFP Considerations for Templating Software**

1. Comprehensive, covering all aspects of a privacy program beyond mere questionnaires
2. Complete content developed by privacy professionals
3. Structured format based on a privacy management framework
4. Include a business case for each privacy management activity
5. 100s of pragmatic spreadsheets, checklists, case studies, template policies and procedures, real world samples, and videos
6. Fully documented revision history
7. Continuous enhancements
8. Search feature
9. Trend analysis of most used resources
10. Reports on the most active privacy management activities, most downloaded resources, and recent updates
11. Where to get started guide
12. Support and training from privacy experts

An effective privacy program includes the appropriate<sup>2</sup> accountability mechanisms from these categories. A good software solution would cover all these accountability mechanisms.

### Templating Software

There are software solutions that provide the Privacy Office with the ability to download not only templates of these accountability mechanisms, but also additional resources. Checklists and real-world examples further enable the Privacy Office to build out and maintain an effective privacy program. Good templating software typically provides:

- Comprehensive coverage of all aspects of a privacy program beyond simple questionnaires
- Complete content written by privacy professionals
- Structured format based on a privacy management framework or a law
- Business cases for each privacy management activity
- 100s of pragmatic spreadsheets, checklists, case studies, template policies and procedures, real world samples, and videos
- Fully documented revision history
- Continuous enhancements
- Powerful search features
- Trend analysis of top downloadable resources
- Top privacy management activity reports
- Recent update reports
- Getting started guide
- Support and training from privacy experts
- GDPR specific templating resources

### The Business Case for Templating Software

Rolling out policies, procedures, and other accountability mechanisms, sometimes referred to as governance, is the only way to mitigate risk, achieve compliance, and demonstrate accountability. Templating software enables risk mitigation, compliance, and accountability. Typically, this is a straightforward business case, due to the time saving when building out a privacy program. With templating software, a more effective program can be implemented in over half the time, without taking any shortcuts.

### Regulator Reporting - Accountability

There is only one way to demonstrate accountability and compliance to regulators, and that is to be able to show that an effective privacy program is in place. Regulators would expect to see policies and procedures that govern the processing of personal data. In some jurisdictions, for example those subject to the GDPR, it is mandatory that you have appropriate technical and organizational<sup>3</sup> measures in place. These policies and procedures form the foundation of the necessary appropriate measures.

### Note on Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are one of the accountability mechanisms typically found in templating software, usually in the form of spreadsheets. These can be sufficient when the amount of personal data processed is low, or the complexity of the processing operations is limited. As will be discussed in Section 3 Automated Privacy Management Solutions, in specific situations a business case can be made for automated PIA software. But most organizations will start with PIAs as spreadsheets prior to automation to ensure their process is effective. Organizations quickly realize that conducting an impact assessment in the absence of a privacy program isn't very effective, and in many cases, the automated PIA implementation is put on hold until a full privacy program is put in place.



<sup>2</sup> What is appropriate will largely depend on the specificities of an organization, including its size and the types and volumes of personal data processed.

<sup>3</sup> Article 24 GDPR

### GDPR Considerations for Templating Software

One of the main requirements under the GDPR is for organizations to implement appropriate technical and organizational measures. What is appropriate, will always depend on the specificities of the organization and the types, volumes, and purposes of data processing. However, the nature of the measures to be taken can be very similar from organization to organization. There is no need to reinvent the wheel when dealing with the GDPR. Either technical and organizational measures that already have been implemented to comply with other laws can be repurposed – and where needed, readjusted – to meet specific GDPR requirements, or inspiration can be drawn from measures taken by other organizations. Templating software is valuable in this respect, since it can help to kick-start the roll-out of a privacy program that is in line with the GDPR, using sample documents that have been specifically developed for this new law. It will also allow organizations to compare their current technical and organizational measures (their accountability mechanisms) with the specific GDPR documents. Finally, the software vendor offering templating software ensures the sample documents are regularly reviewed to ensure the most current legal requirements, regulator guidance, and court decisions are taken into account, thus again saving the Privacy Office time and effort.

Nymity's Templating Software Solution is:



NYMITY  
TEMPLATES™

Privacy Templates and Checklists to Help Structure Privacy Programs



ASK ABOUT OUR  
GDPR ADD-ON

## Planning Software

In larger organizations, a privacy program is often managed by a team of individuals, the Privacy Office. Only recently has software been developed to help the team plan, maintain, and report on a structured privacy program. Historically the Privacy Office had to use spreadsheets, portals, emails, and other generic office software to support their efforts.

*Planning software enables better:*

**Program Visualizations:** Good planning software typically provides a dashboard that enables quick visualizations of the privacy program status and outstanding activities and deadlines. This makes for better communications and better resource allocations.

**Program Resourcing:** Privacy management activities are continuously being completed by the Privacy Office team. Planning software allows the Privacy Officer to monitor and plan privacy management activities, can save time, and can help to ensure an effective privacy program is indeed developed.

**Gap Assessments and Mitigation:** Planning software allows for the documenting of the current status of the privacy program plus the plans going forward, including any gaps identified. Resources are then applied to the identified gaps including the necessary reporting and accountability requirements.

**Program Reporting:** Good planning software will provide regular, as well as on-demand reporting on the progress of privacy program implementation and maintenance. This is not only good for planning purposes, it also supports management reporting and the demonstration of accountability to all stakeholders, including regulators. Good reporting helps justify the Privacy Office resources, and in some cases, helps make the business case for more resources.

## The Business Case for Planning Software

Often the business case for planning software is better resource management, reporting, and maximizing accountability. This is typically due to the fact that most Privacy Offices are made up of non-dedicated individuals that report into different parts of the organization. Planning software enables better maintenance of a privacy program.

Ultimately, a well working Privacy Office enables an effective privacy program which results in maximized risk mitigation, compliance, and demonstrable accountability. Some also include in their business case the better use of resources, namely the time involved of individuals on the Privacy Office team.



### RFP Considerations for Planning Software

1. Flexible, customizable structured format based on a privacy management framework
2. Interactive dashboard of status and details of privacy program
3. Ability to attribute statuses to privacy management activities: Implemented, In-progress, Desired, N/A
4. Owner management for accountability
5. Filters based on GDPR, OECD principles, BCR, APEC-CBPR, and other common privacy frameworks
6. Ability to document evidence of privacy program
7. Free user licensing for law firms and consulting firms
8. Monthly privacy management reports
9. Task management
10. Full audit history
11. Getting started guide
12. Support and training from privacy experts
13. Demonstrate accountability of the privacy program and the team
14. Filter based on privacy team, priorities, mandatory activities, % complete

### GDPR Considerations for Planning Software

The GDPR requires organizations to be able to demonstrate they comply with the requirements of the law. This is called the accountability principle, which is enshrined in Article 5. In order to do so, some form of documentation on the development of a privacy program is required. Planning software can help in that regard, because it assists the Privacy Office in documenting what steps are taken by which team member when developing, implementing, and maintaining a privacy program. Ideally, it also allows for the inclusion of relevant documentation (for example project documents, minutes of meetings, and drafts of the appropriate technical and organizational measures to implement), in order to ensure everything can be retrieved from the same place, should questions be asked.

Nymity's Planning Software Solution is:



NYMITY

PLANNER™

Tools to Plan, Build, and Embed Privacy Management Across the Organization



ASK ABOUT OUR  
GDPR ADD-ON



## Benchmarking Software

Management generally does not only want to be kept up-to-date on the development of the internal privacy program, they would also like to understand where the company stands in comparison to other organizations. In some cases, they would like to compare one part of the organization to another. In other cases, they want comparisons based on industry, size, and location. Benchmarking software will allow for these comparisons. Good benchmarking software will also allow for functions that go beyond the comparisons.

**Readiness Assessments:** Good benchmarking solutions include the reporting on the status of privacy management within the context of readiness assessments, for example to the GDPR, Binding Corporate Rules (BCR) or other frameworks such as the APEC Cross Border Privacy Rules (CBPR). This helps to clearly identify gaps, and allows management to assess where resources are needed to support compliance efforts.

**Management Reporting:** Good benchmarking software will include a suite of reports that can be used for management reporting at either regular intervals or on-demand. Good reporting helps to justify the Privacy Office resources and in some cases, helps make the business case for more resources.

### The Business Case for Benchmarking Software

Understanding what other organizations are doing for privacy management enables better planning and resource allocation. Often, benchmarking software itself is used for management reporting or business cases that justify further investments in privacy management. In some cases, the benchmarking is justified in the same business case as the planning software.



#### RFP Considerations for Benchmarking Software

1. Standard privacy management comparative framework
2. Empirical measurements
3. Standard definitions and scopes of comparative activities
4. Create custom comparative charts
5. Receive relevant comparative reports monthly
6. Summary comparisons or detailed activity-based comparisons
7. Reports based on risk mitigation activities
8. Ranking reports providing listings of top privacy management activities
9. Support Readiness Assessments, for example to GDPR or other frameworks or laws
10. Full training and support by privacy principles

### GDPR Considerations for Benchmarking Software

As explained before, the GDPR requires organizations to implement appropriate technical and organizational measures. But where to start when you want to find out what is appropriate for your own organization? In such situations, benchmarking software can support you. Not only does it provide an easy way to complete a gap assessment of your current privacy program, ideally checked specifically against the requirements of the GDPR, but it also allows you to compare your GDPR readiness with that of other organizations. If the reporting is detailed enough, benchmarking software could provide insights in what peer organizations in your region or sector are considering to be appropriate measures, allowing you to draw inspiration to enhance your own program.

Nymity's Benchmarking Software Solution is:



NYMITY

BENCHMARKS™

Privacy Program Benchmarking and Insightful Comparisons



ASK ABOUT OUR  
GDPR ADD-ON

## Section 3: Automated Privacy Management Software

Privacy management software has been around for many years, but recently there have been some interesting innovations. Historically, privacy management software solutions were basic automated questionnaires with some workflow elements and simple reporting. With recent advancements in data visualizations, expert systems, business intelligence, and next generation reporting, privacy management software implementations are much more successful.

Other innovations in privacy management software leverage the advancements in organizational accountability, including the implementation of effective privacy programs. Now, some of the new software that is coming to market take advantage of organizational investments in privacy programs.



*“Perhaps the biggest takeaway from this year’s survey, however, is the role that technology is now playing in privacy management. The second most popular tool for GDPR preparation is investing in technology: 55 percent of respondents plan to make such investments, compared to just 29 percent last year. Among privacy team duties, the use of privacy-enhancing software rose to 31 percent of respondents from 24 percent in 2016.”*

IAPP-EY Annual Privacy Governance Report 2017



### What is Privacy Management Software?

Privacy management software allows the Privacy Office to engage the business directly through some form of automated questionnaire and/or expert system. The three most common elements are privacy impact assessments (PIAs)/data protection impact assessments (DPIAs), data mapping/data inventory, and enterprise assessments.

#### Are there Prerequisites for Privacy Management Software?

Privacy management software typically works best when a privacy program has been deployed in the organization, which makes sense. After all, how can you implement privacy management software without a privacy program? Some organizations will conduct an initial privacy assessment, often referred to as a readiness assessment. In those cases, some use a software solution, while others use spreadsheets. It is difficult to create a business case for one-time readiness assessments, but ongoing enterprise assessment software can have a strong business case in certain situations, discussed below.

#### When is Automation Required?

Generally, there are two factors to consider when deciding when to acquire software solutions:

##### 1. Volume

Do you have sufficient volumes of privacy management activities that justify the acquisition of a software solution? For example, if your organization conducts less than 20 PIAs/DPIAs per year, a simple spreadsheet might suffice. Software is generally justified in higher volume situations as it will result in time and resource savings.

Complexity	High Complexity	Software can Help	Software is typically Required
	Low Complexity	Spreadsheets are Sufficient	Software can Help
		Low Volume	High Volume

2. Complexity

How complex are your business processes? Complexity could come in the form of vast types of processing activities, multiple locations of business, high-risk technical processing, and complicated legal obligations. When the complexity is high, a good software solution can help address your needs. This is especially true for software solutions that have legal obligations built-in, as some of the next generation software solutions do today.

# 1 Criteria for Software Selection = Business Engagement

Although not obvious to first time buyers, one of the critical success factors for any privacy management software is the level of engagement with the business. When selecting a software solution, it is best to select one that can work well with all four levels of business engagement (see table below). Selecting a software solution that relies on a “Privacy Champion” in the business will significantly decrease the probability of a successful implementation. It is unlikely that “Privacy Champions”, who maintain privacy knowledge and are motivated to complete the assessments, will be present in all business units. The following chart illustrates the four levels of business engagement that privacy management software should be able to work with, regardless of what level is presently achieved. Organizations should also bear in mind that the level of business engagement can vary from department to department, and may change over time.

Business Engagement	Attributes	Privacy Office
Limited	May review a report	Privacy Office is the only user
Responsive	Attend a webinar, a meeting, a phone call, reply to email	Privacy Office is the only user
Engaged	Will use software when directed but have limited interest in privacy	Business uses software, Privacy Office adds a lot and changes a lot
Champions	“Privacy Champions” Proactively will use the software without prompting and have some knowledge in privacy	Business a heavy user with Privacy Office providing mostly oversight

This Buyer’s Guide will look at the most common types of Privacy Management Software for the Privacy Office.

- 1 Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) Software
- 2 Data Mapping/Data Inventory Software
- 3 Enterprise Assessment Software

## Privacy Impact Assessment (PIA)/Data Protection Impact Assessment (DPIA)

A traditional PIA is a risk assessment conducted on a new or substantially enhanced processing of personal data. Historically, PIAs were structured based on a set of processing-related questions to identify attributes of risk to the processing which could then be mitigated.

DPIAs are sometimes used interchangeably with PIAs, but increasingly DPIAs are being considered as a secondary assessment or additional assessment when it is deemed that the processing involved is likely to be of high risk in nature. This is largely due to how the GDPR defines the criteria for conducting a legally mandated DPIA.

PIAs have been around since the 1980s, and automated solutions have tended to automate the traditional approach to PIAs, i.e. questionnaire-based surveys. Recent advances in PIA automation have created innovative new approaches, lending themselves to greater efficiency and scalability. At the core, PIA software has the following functionality:



### Questionnaires

Standard question sets which are sometimes based on publicly available PIAs from regulators and other government authorities, or the repackaging of a law into a series of questions. Some have threshold questionnaires designed to identify if there is a likelihood of high risk processing that would indicate the need for more questions to be asked, often in the form of another questionnaire.



### Approval Process

A workflow where one or multiple individuals are involved in the approval process, based on the identification of risks and defined actions that would need to be completed prior to approving a project.



### Risk

The ability to identify risk, generally at the question level, as well as functions to document and monitor mitigation strategies.

### RFP Considerations for PIA/DPIA Software

1. Expert System with auto-learning
2. Automatically identify high risk triggers (DPIA)
3. Expert threshold assessment
4. Automatically trigger DPIA without Privacy Office involvement
5. Full purposes knowledgebase
6. Full data subject knowledgebase
7. Full data type knowledgebase
8. Full accountability mechanism knowledgebase
9. Quick approval process
10. Detailed approval process
11. Automatically map appropriate accountability mechanisms to projects
12. Automatically trigger Privacy by Design guidelines/checklists and oversight
13. Support pre-answered questions with oversight
14. Regulator reports updated based on regulator published expectations
15. Custom regulator reports setup by Privacy Office
16. Custom management reports
17. Full training and support from privacy professionals

## Next Generation PIA/DPIA Software

In addition to core functionality, it is worth looking at some of the advancements that are taking place in PIA/DPIA software as these advancements can substantially increase risk mitigation while increasing the speed and increasing the accuracy of the PIA/DPIA. These software advancements include:

1. **Auto-High Risk (DPIA) Triggers.** Identifies high risk processing either as defined by law (e.g. GDPR), by regulators, or defined by the Privacy Office. This automatically informs the Privacy Office of high risk processing. Some software systems can also automatically add DPIA questions or even pre-defined actions when high risk is identified, substantially reducing the burden on the Privacy Office and the overall duration of the PIA/DPIA process.

---

2. **Auto-Accountability.** Triggers specific policies and procedures to be followed during the PIA/DPIA process, thus baking accountability right into the PIA/DPIA process. Not only does this substantially reduce risk, it aligns well with agile development and ensures ongoing awareness of policies and procedures resulting in demonstrable accountability at a PIA/DPIA level.

---

3. **Auto-PbD.** Specific organizational Privacy by Design (PbD) and default controls that are triggered for processing that requires PbD. Checklists and other instructions are embedded right into the PIA/DPIA process which is powerful from a reporting standpoint.

---

4. **Regulator Reporting.** Out-of-the-box regulator reporting that are automatically tailored to the regulator's changing expectations. It is not uncommon to have multiple regulator reports for a single regulator. Also, some software solutions allow for customers to tailor their regulator reporting for their specific desires.

---

5. **Benefits to Individuals.** Goes beyond risk, and incorporates functions to capture benefits that individuals may receive from the processing of their personal data. This functionality provides more complete regulator reporting and improves management reporting. It will also support organizations wanting to demonstrate that their data processing is meeting certain ethical standards.

---

6. **Expert Content.** Prepopulated with the necessary expert content to support the Privacy Office during the PIA/DPIA process. For example, these software solutions contain all of the purposes for processing personal data, data types, data subjects, and other key information out-of-the-box.

---

7. **Expert Systems.** Learn from past PIAs/DPIAs in order to predict, and in some cases, prepopulate necessary information for a PIA/DPIA. The system gets smarter as more and more PIAs/DPIAs are completed.

---

8. **Multiple Approval Functions.** Options for handling the approval process can include auto-approvals of PIAs when they meet certain criteria. Quick approval processes completed at the PIA/DPIA level, or more detailed question-based approval processes.

---

9. **Pre-Answered Questions.** In some cases, legal-based questions can be pre-answered and reviewed only by the Privacy Office. For example, when companies have internal standards that are relevant to most processing activities, the answers can be created once, used often, and only adjusted in the rare circumstances in which the standard is not followed.

---

10. **API-PIA.** Application Programming Interface (API) allows for the automation of data imports and exports from the PIA solutions. In some cases, the PIA software will integrate with APIs of other PIA vendors, providing a rapid migration path from one PIA software vendor to another, or with other organizational management solutions, like GRC tools.



## GDPR Considerations for PIA/DPIA Software

A responsible organization has to have an understanding of the risks to the rights and freedoms of data subjects its data processing operations may cause. Article 35 of the GDPR specifically mandates that in case of high risk, a Data Protection Impact Assessment needs to be completed. Such a DPIA requires an organization to identify the risk involved in processing personal data, as well as to subsequently mitigate the risk to the rights and freedoms of the data subject. In case of non-high risk processing, an impact assessment is not mandated by law, but would still be regarded as a best practice.

Many organizations will only have a limited number of processing operations, maybe one or two of which would be considered high risk. In such situations, impact assessments that are based on spreadsheets or other simple documents will generally suffice. However, especially in case of what is referred to before as high volume or high complexity data processing operations, PIA/DPIA software could be especially useful when dealing with the GDPR. Good PIA/DPIA software will be able to identify for each of the EU Member States – and other countries– if the risk of the processing operation is to be considered high. That could be on the basis of the GDPR itself, or the guidance from the Article 29 Working Party, but it could also be on the basis of specific national laws and local regulator guidance. Another important advantage of using PIA/DPIA software, is that it will become easier to keep your impact assessments up-to-date. This is required under the GDPR, as clearly explained by the Article 29 Working Party in their Opinion 248<sup>1</sup> on the Data Protection Impact Assessment.

<sup>1</sup> [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611236](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236)

Nymity's PIA/DPIA Software Solution is:



**NYMITY**  
**EXPERTPIA™**

Tools to Produce Fast and Accurate Accountability-based PIAs



**ASK ABOUT OUR  
GDPR ADD-ON**

## Data Mapping/Data Inventory Software

There are many forms of data mapping and data inventory software, but what is emerging as the most common is compliance data mapping software. Data mapping for compliance is often driven by regulator reporting and requires an organization to identify where data is collected in a specific jurisdiction, where it is processed, the types of data and the data subjects involved, when collection or processing occurs outside that jurisdiction, and the legal grounds for a data transfer. In some jurisdictions, for example in countries subject to the GDPR, there is a legal obligation to produce a record of processing activities, and if high-risk processing occurs, a Data Protection Impact Assessment (DPIA). This can all be accomplished with a comprehensive compliance data mapping solution when designed for that purpose.

Data mapping starts with the documentation of data type by jurisdiction. Keeping data mapping simple is critical to its success and key to be able to quickly demonstrate:

1. Where personal data is collected, and
2. Where personal data is being processed

When the location for the collection and processing is different, the software needs to provide the legal grounds for the data transfers, either within the organization or to third parties.

Visualizations are a critical component of compliance data mapping software. Visualizations should allow for easy identification of processing specific data types (e.g. sensitive data), purpose of processing, data recipients, legal grounds for transfer, and a wide variety of other attributes. Compliance data mapping software should support regulator inquiries and any local regulator reporting. This includes, for example, an Article 30 GDPR records of processing activities report.

Advanced time-saving functions provided by some compliance data mapping software include:

- 1. PIA/DPIA Integration.** Integration with PIA/DPIA software, allowing for a single set of questions and/or an expert system to capture the necessary information for both the PIA/DPIA and the data mapping. For customers that require both functions, this saves a considerable amount of time by avoiding duplication of work.
- 2. Expert Content.** Prepopulated with the necessary expert content to support the Privacy Office during the data mapping process. These software solutions contain all of the purposes for processing personal data, data types, data subjects, and other key information out-of-the-box.
- 3. Expert Systems.** Learn from past data mapping in order to predict, and in some cases, prepopulate necessary information for a data mapping. The system gets smarter as more and more data mapping is completed.
- 4. Data Subject Rights Requests.** Help the Privacy Office manage data subject rights requests by quickly identifying the locations and data types of the processing of individual personal data.



### RFP Considerations for Data Mapping Software

1. Expert System with full content out-of-the-box
2. Auto-learning
3. Regulator reporting
4. Custom regulator reporting
5. Optional PIA/DPIA integration
6. Support data subject access requests
7. Support data breach
8. API to other systems
9. Full business intelligence visualizations
10. Full support and training from privacy professionals

5. **Data Breach Support.** Functions that help the Privacy Office manage breach events by identifying data types that would be subject to the breach.
6. **API.** Application Programming Interface that allows for existing information to be imported (or exported).

### GDPR Considerations for Data Mapping Software

Data mapping as such is not a phrase you will find in the GDPR. However, the Regulation does put an obligation on organizations to keep a register of all data processing operations that can be made available upon demand to the data protection authority. Many organizations assume that such a register can only be built on the basis of a full data inventory and data mapping exercise, which needs to be software-based.

Although there are differences between a data inventory or data mapping exercise on the one hand, and establishing a processing activity register on the other hand, data mapping software can help to establish the required register. When organizations map their data processing operations across the world, but especially those in the EU, it is not so difficult to include at the same time all the information that is required by Article 30 GDPR for the processing activities register. The register would then simply be an output of the data mapping software, which would indeed be available on demand, and moreover, be up-to-date as long as the data maps are regularly reviewed. As is the case of PIAs/DPIAs, automating data mapping only has a viable business case if the data processing within an organization is high volume or high in complexity. If not, a spreadsheet would again suffice.

Another advantage of data mapping software in light of GDPR would be a clear overview of all non-EU data transfers, allowing organizations to make an assessment of what data transfer mechanisms might be best suited. Visualizations could provide an indication that it would be worthwhile to apply for a Privacy Shield certification, based on increased data transfers to the U.S., or for Binding Corporate Rules, based on high volumes of intra-company data transfers, of which the Privacy Office may not have been aware.

Nymity's Compliance Data Mapping Software Solution is:



NYMITY

EXPERTMAPPING™

Expert Solutions for Processing Data Inventory and Data Mapping



ASK ABOUT OUR  
GDPR ADD-ON

*Note: BigID, Integris, and Prifender offer automated data discovery solutions that integrate well with Nymity's compliance data mapping software.*

## Enterprise Assessment Software

Enterprise assessment software, sometimes incorrectly referred to as readiness assessment solutions, are typically a repackaging of Privacy Impact Assessment software with a different questionnaire. This is due to the fact that it is common to start off a compliance project with a readiness assessment. The problem is that readiness assessments are just that - readiness assessments. They do not work well as ongoing enterprise assessment software, as they are designed for one-off assessments. What is required is a software solution that is designed for ongoing enterprise assessments, much like audit software works.



### Enterprise Privacy Assessments are Unique

Over the years, organizations have tried to use security and other IT solutions to conduct ongoing assessments, generally based on controls. Privacy compliance tends not to fit well into these types of solutions for a variety of reasons. What has evolved are software solutions that were designed specifically for privacy.

### Accountability

The key to enterprise assessment software is accountability, specifically a structured approach to demonstrate an ongoing effective privacy program, implemented across the organization. As such, an ongoing or annual assessment of a privacy program across an organization is becoming more common. In some cases, these accountability-based assessments are being conducted to satisfy a requirement in Binding Corporate Rules (BCRs), an optional legal ground for data transfers found in the EU and now codified in the GDPR. In other cases, they are being conducted to fulfil obligations found in a US consent decree or as part of privacy program governance. GDPR also has a requirement for being able to demonstrate ongoing compliance, which will likely result in an increase in enterprise assessment software implementations once organizations have privacy programs in place that can be assessed.

The traditional approach to conduct an enterprise assessment is to ask a series of questions, which an expert would then review, use to identify risks, and mandate/recommend risk mitigation actions. This traditional approach often leads to the same software used for PIAs to be used for enterprise assessment, with a different set of questions. Essentially, the organization is conducting a readiness assessment over and over again with some history functionality. All enterprise assessment software should be able to conduct this function, but there are new advances worth considering.

### Next Generation Enterprise Assessment Software

Recent and more advanced software solutions to conduct enterprise assessments include functions such as:

#### RFP Considerations for Enterprise Assessment Software

1. Historical reporting
2. Not a repackaged PIA solution
3. Build on accountability (privacy program)
4. PIA/DPIA integration
5. Attestation-based and audit-based
6. Legal expert system mapping evidence to laws
7. Allow weighting for reporting high risk parts of the business having a higher impact on the accountability scoring
8. Full training and support from privacy professionals

- 1. Historic Dashboard Visualizations:** The capability to graphically track historical changes in the overall maturity and status of accountability across the organization. This is important for communicating with management and standing-ready to communicate with regulators. The visualizations are important as they allow for effective communications to non-privacy experts about privacy accountability and compliance.

2. **Comparative Reports:** Allow for different parts of an organization to compare themselves with other parts. This can also be done from an historical standpoint. It not only enables better communication, it fosters a competitive nature between parts of the organization, helping to further mitigate risk.
3. **Attestation-Based:** Provides the business with the ability to quickly attest to specific program compliance using fast assessment functions and meaningful visualizations.
4. **Risk-based Scalability:** To enable high-level assessments at lower risk areas of the organization and more in-depth assessments at high risk procession not only at a reportable unit level, a questionnaire level, but in the depth of evidence that is required.
5. **Evidence-Based:** Provides different forms of evidence to help the business easily verify their attestations. This evidence can be quite helpful when conducting a deeper risk review or when supporting a regulator inquiry.
6. **Program-Based Evidence:** Why have the business load evidence when they simply need to verify they are following and applying the policies, procedures, and other accountability mechanisms that are in place for the privacy program? In other words, the privacy program is the evidence, but its application has to be verified by the business.
7. **Educational:** Software that builds the assessments based on the privacy program goes beyond enterprise assessment, as it results in the business maintaining knowledge of the policies and procedures on which the program is built.
8. **Audit-Based:** Allows Privacy Offices or audit departments to challenge the business, requiring a second level of verification.
9. **Legal Expert System:** The ability to map evidence that is collected during an assessment process to rules of law. This type of software requires the maintenance of the over 700 privacy laws around the world. The software then becomes a huge time-saving tool for jurisdictional compliance. Plus, it allows for evidence-based demonstration of compliance to laws.
10. **PIA/DPIA Evidence Integration:** Direct integration with PIA solutions at the evidence layer. Software providers that recognize that there is only one privacy program enable an organization to successfully document the privacy program in a manner that it can be used for evidence in both the PIA/DPIA and the enterprise assessment software.
11. **PIA/DPIA Reporting Integration:** Provides a reporting structure based on a common organizational structure. This can save significant time and enhance communications as it allows for common reporting structures between the processing of personal data and the privacy program infrastructure in place to govern the processing of personal data.
12. **Custom Reporting.** The ability to set up custom reports for different parts of the organization and have them run at different intervals.
13. **Flexible Assessments Timing.** Allows for different parts of an assessment to be assessed at different times. These software solutions provide extra flexibility by allowing quarterly quick assessments for more dynamic privacy program functions, and annual assessments for the less dynamic functions.
14. **Proactive Reminders.** Solutions will automatically send reminders for annual or ongoing assessment, in advance of the assessments, either at a question or at an assessment level.
15. **Evidence Management.** Functions that provide evidence status reports enabling the management of evidence of the privacy program used in the enterprise assessments.
16. **Weighting.** The ability to increase weighting to areas of higher importance, which are in turn reflected in the assessment score. For example, a business unit that conducts 75% of the processing can be configured to have 75% of the total weighting.
17. **Business Intelligence.** Allows the organization to visualize their data in a way that provides insight back to the business, improving the decision-making process.



### **GDPR Considerations for Enterprise Assessment Software**

Under Article 24 GDPR, organisations are not only required to take appropriate technical and organisational measures to ensure compliance, but these measures also need to be reviewed and updated on a regular basis. An organisation could therefore benefit from enterprise assessment software to keep track of their capacity to comply, as well as the implemented technical and organisational measures, at all levels of the organisations. An easy dashboard should provide an overview of the historical and current status, as well as review requirements. Once set up, enterprise assessment software will not only support organisations to demonstrate compliance with the GDPR, but also with other laws and even with internal privacy policies, like Binding Corporate Rules.

Nymity's Enterprise Assessment Software Solution is:



NYMITY  
**ATTESTOR**™

Quantitative and Qualitative Analysis to Demonstrate Compliance



ASK ABOUT OUR  
GDPR ADD-ON

## Section 4: Software Vendor Considerations

When selecting a vendor for privacy software, there are a number of attributes that should be taken into consideration, including:

1. **Demonstrable Privacy Expertise.** Does the software provider have demonstrable in-depth knowledge of privacy? How long? Expertise takes the form of full-time dedicated employees and content or publication of thought leadership materials, such as frameworks and methodologies.
2. **Depth.** Check the depth of knowledge, the currency, the accuracy, the history, and the number of law firms that rely on the vendors content.
3. **Customer Success.** Does the software provider have a dedicated team of privacy professionals that support the software solutions? This can be quite important to obtain relevant and effective training and support.
4. **Track Record.** How many years in the field of privacy management do they have? How many employees do they have that have been with the company for over 10 years? Do they have a sustainable structure for the future?
5. **Regulator Research/Reporting.** Does the software provider have a demonstrable history of working with regulators, not only in republishing their materials as content, but by being involved in projects that benefit the regulators, the regulated, and ultimately the data subjects? It would be beneficial to have former senior regulatory privacy experts working at the company.
6. **Customer Loyalty.** Can the software vendor provide a list of long-term customers that have renewed for many years?
7. **Portability.** Does the software provider lock you into long-term contracts or not provide an easy migration path to other vendors?
8. **Mandate.** Is the software provider's mandate in line with the objectives of the Privacy Office?
9. **Law Firms and Consulting Firm Partnerships.** Does the software provider have a strong working relationship with all individuals that support the Privacy Office for compliance? Do they have special software licensing that enables their customers to easily work with their chosen law firm and consulting firm?
10. **Global Focus.** Does the software provider primarily focus on GDPR, trying to leverage the current trend, or are they focused on privacy compliance in all jurisdictions? GDPR is important but there are many other privacy laws that organizations need to comply with, and there are many more laws or changes of laws coming in the future.
11. **GDPR.** Has the vendor been preparing to support its customers since the GDPR was officially announced in January 2012? GDPR may seem new but most of the legal obligations are near their original form from over six years ago.
12. **Works with Regulators.** Has the software provider been working with, and gaining intelligence from privacy regulators? It is necessary to understand what regulators consider important, such that the software solution inherently builds in functions that satisfy regulator needs and expectations.



*"Buyers should be vigilant about the potential future of a product. In some cases, a start-up getting bought out by a larger company with more features will benefit the buyer. In others, the buyer may experience a dead end."*

IAPP 2017 Privacy Tech Vendor Report



## Section 5: About Nymity: Privacy Compliance Software, Powered by Expert Research

Nymity was incorporated in 2002 to support the Privacy Office. At that time, in Canada (where Nymity's head office is located) a private sector privacy law went into effect. The law, The Personal Information Protection and Electronic Documents Act (PIPEDA), was the first in the world to have an accountability principle that included an obligation to have an individual or individuals responsible for privacy. In other words, a Privacy Officer was required by law. Nymity's mandate was, and has been ever since, to support the Privacy Office. For over 15 years, we have done so at a global level, by developing state-of-the-art research-driven software solutions.

It was as clear in 2002 as it is today, that the foundation of any privacy software has to be deep privacy knowledge. As such, the first division of Nymity was a Research Division made up of privacy professionals that are dedicated to conduct compliance research on privacy laws. Privacy knowledge is the foundation of all Nymity's software solutions. This dedication has made Nymity the #1 research-based privacy compliance software vendor in the world. No other software vendor has the depth in knowledge supporting their software.



*"Nymity, which operates in its own market category in a sense, uses deep research of data protection laws and regulations to offer software, templates, assessments, and compliance strategies to help implement and maintain a functioning Privacy Office. They also work with regulators to help improve compliance and accountability."*

IAPP 2017 Privacy Tech Vendor Report

### #1 Research-Based Privacy Compliance Software for the GDPR and the World's Privacy Requirements



#### Legal Research Software

Understand the ever-changing privacy compliance obligations and expectations around the world.



#### Privacy Office Support Software

Build/maintain a demonstrably compliant privacy program that results in ongoing compliance.

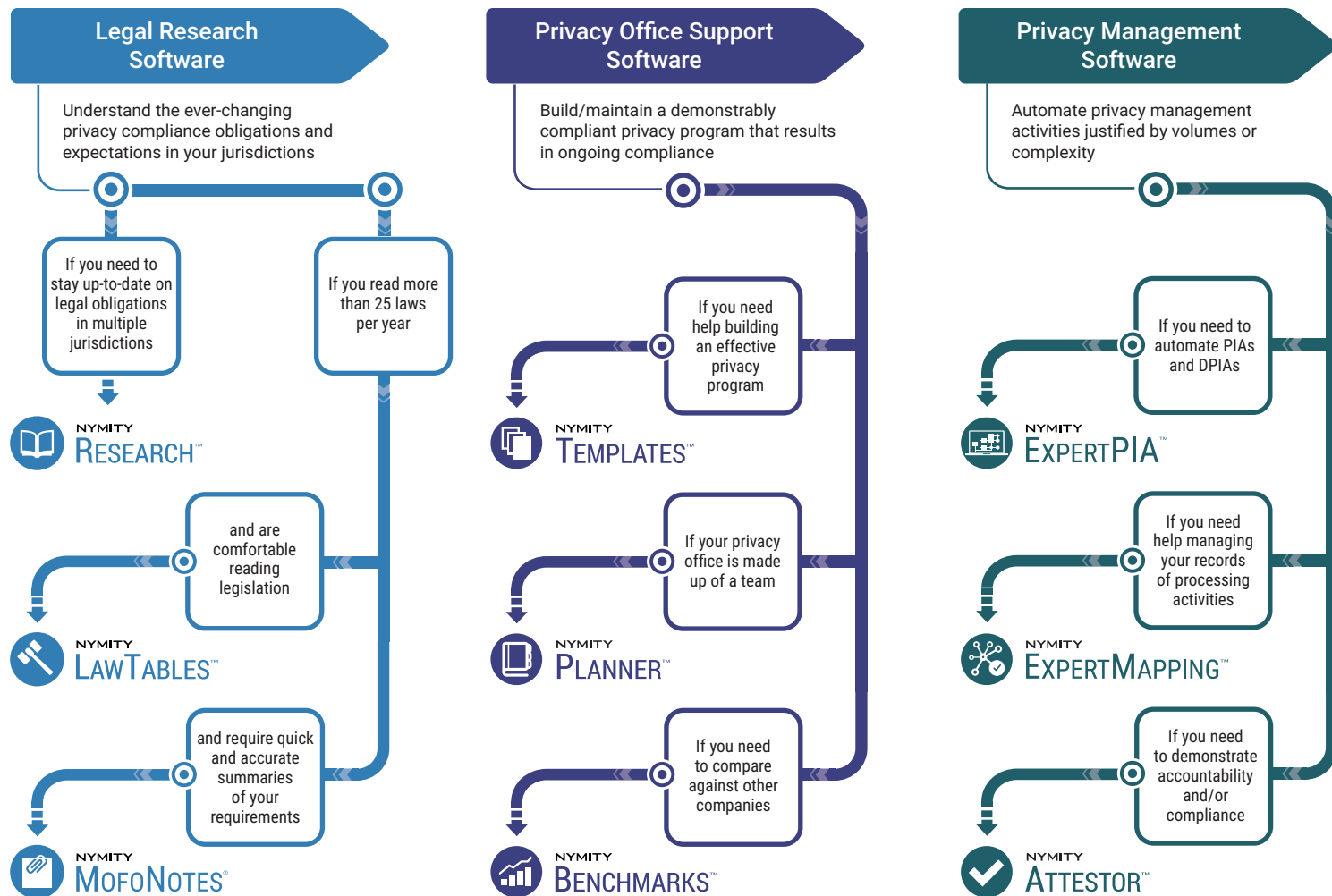


#### Privacy Management Software

Automate privacy management activities justified by volumes or complexity.



# Software Solutions to Empower the Privacy Office



## Nymity and the GDPR

Nymity supports over 700 privacy laws from across the globe. This includes the GDPR, as well as the national laws in the various EU Member States that supplement the GDPR. We have been working on GDPR compliance for over seven years, first conducting workshops with the European Commission on accountability during the drafting phase, and subsequently preparing our solutions for the Regulation from the moment a first draft was leaked in November 2011.

All Nymity's solutions for the Privacy Office take an accountability approach, and allow for easy maintenance and monitoring of a privacy program, as well as turn-key reporting on compliance. From that perspective, the GDPR is "just another law" that needs to be complied with. Our solutions will help your organization do exactly that: comply with the GDPR, while at the same time supporting compliance with all the other privacy laws you may be subject to.

Copyright ©2018 by Nymity Inc. All rights reserved. This document is provided "as is" without any express or implied warranty. This document does not constitute legal advice and if you require legal advice you should consult with an attorney. Nymity may not have addressed all legal requirements applicable to your organisation and the document may need to be modified in order to comply with relevant law. Forwarding this document outside your organisation is prohibited. Reproduction or use of this document for commercial purposes requires the prior written permission of Nymity Inc.



# PRIVACY COMPLIANCE SOFTWARE

*Powered by Expert Research*

[WWW.NYMITY.COM](http://WWW.NYMITY.COM)