NYMITY
innovating compliance

2018 PRIVACY COMPLIANCE SOFTWARE

BUYER'S GUIDE

NYMITY
GDPR Edition

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.[1] 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.

GDPR

Also, the Buyer's Guide will address how software can help with ongoing compliance with the EU General Data Projection 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

[1] https://iapp.org/resources/article/2017-privacy-tech-vendor-report/

Software for the Privacy Office

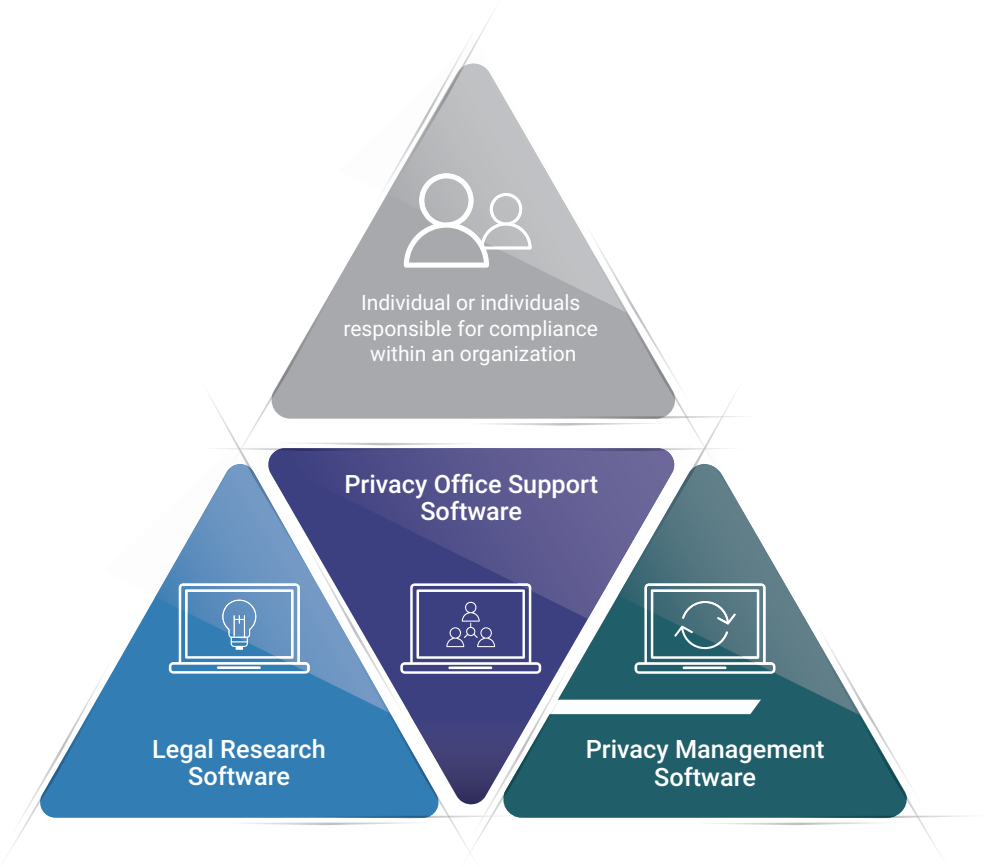
Since the first privacy laws, many organizations have assigned one or multiple individuals to maintain compliance with privacy laws, often called the Privacy Office or a Data Protection Officer (DPO). They need:

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

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

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

PRIVACY COMPLIANCE SOFTWARE

Powered by Expert Research

WWW.NYMITY.COM