

Knowledge Brief

Quadrant Knowledge Solutions

Syrenis is Leader in SPARK Matrix: Privacy Management Software, 2022



An Excerpt from Quadrant Knowledge Solutions
“SPARK Matrix: Privacy Management Software, 2022”

Syrenis is Leader in SPARK Matrix: Privacy Management Software, 2022

Privacy Management Software enables organizations to store sensitive data in compliance with privacy regulations, analyze the data flow of personal information, assist in the distribution of privacy policies, and utilize confidential data ethically and effectively. The software helps users automate complex privacy management activities such as privacy impact assessment, examine processing activities against privacy regulations, and monitor the business processes accountable for the unlawful disclosure of personal data in an organization.

Due to the increasing awareness and advocacy of customers, organizations should be cautious while storing personal information, particularly with the growing need to provide customers with information about the ways in which their data is handled and stored. Companies are struggling to manage and adhere to compliances with different privacy regulations around the world, the growing concerns associated with personal and sensitive data breaches, and the country-wise growth of various privacy frameworks and regulations, thereby generating the need for adopting different privacy solutions. The data privacy management software helps organizations manage and store customers' data in accordance with global privacy legislation such as General Data Protection Regulation (GDPR), California Consumer Protection Act (CCPA), and Health Insurance Portability and Accountability Act (HIPPA).

A privacy management platform continuously detects, analyzes, and determines the regulations that are likely to be applicable within an organization's privacy requirements based on multiple factors like location, size, and domain of operation. It creates a central inventory of data flow and processes and consolidates and centralizes the personal information, consent, and preferences of each data subject gathered by the organization into a single repository. A privacy management software thus assists enterprises in mitigating the risk of data loss or theft and unauthorized data access.

Privacy management software vendors offer key functionalities such as assessment automation that operationalizes privacy impact assessments (PIAs), data protection impact assessments (DPIAs), privacy by design (PbD), and other

internal privacy and security assessments. Furthermore, data mapping and flow assist users in determining the flow of data through an organization, and privacy rights management automates the data rights request management. It also helps organizations quickly respond to users and automates requests from intake through fulfillment, including data discovery and redaction of sensitive information, are some other significant functionalities of the software. Also, the incident management capability in privacy management software centrally manages the data or security breach incidents, auto-generates the guidance, and automates root cause analysis to reduce the chances of similar incidents repeating themselves. Furthermore, the policy and notice management eliminates the tedious process of generating, updating, and monitoring policies across websites and applications, and instead consolidates them into a single location, while the consent and preference management functionality helps in collecting and managing personal information in accordance with regulatory compliances.

Some industry verticals, including banking, financial services, information technology, telecommunication, government, and healthcare, extensively adopt privacy management software to protect the users' sensitive data and maintain data privacy compliance in accordance with multiple regulations. While most privacy management software vendors provide comprehensive functionalities to support multiple emerging use cases to meet the organizational needs of deploying compliance-based privacy solutions, their technology and customer value proposition may differ based on the customer size, industry vertical, geographical markets, and organization-specific requirements. Some of the key competitive factors and technology differentiators where users should evaluate and compare various privacy management software vendors include their ability to offer support to a wide range of pre-packaged use cases, the solution's integration and interoperability, product strategy, and roadmap, and sophistication of technology offering.

Market Drivers

- The privacy management software market is growing rapidly, as the industries are focusing on safeguarding their confidential information from theft and controlling unauthorized access to the data.
- Due to the COVID-19 pandemic, global businesses and workplaces switched their work models to remote working in order to keep functioning. This amplified the problem of cybersecurity and cyber

breaches since privacy was a major concern from the employee's end.

- Global data privacy and security frameworks are growing in order to maintain regulatory compliance with different data protection policies and laws. End users are more cautious about the usage of their personal data by organizations and are hence increasingly adopting privacy management software to keep a tab on the accurate inventories of data.
- Organizations are embracing the bring your own device (BYOD) concept to provide employees with the flexibility of work. This drives the need for regular open networks that are secured so that employees can access official data through their personal systems.

Technology Drivers

The technology trends that are driving the growth of the privacy management software market are:

- Enterprises are largely focusing on data privacy automation to be transparent and efficient. They are looking to automate various privacy activities, including records of processing activities, third-party risks, legislative compliance, data subject access request management, and consent preference management.
- To eliminate complex manual, and time-consuming data subject access request (DSAR) responses, the organizations are mainly focusing on the implementation of DSAR management in privacy management software to dynamically assess requests and securely deliver accurate and quick responses to a large number of data subjects.
- Multiple threats and vulnerabilities arise due to insecure interfaces in relation to the applications, protocols, and services required for communication. Most of these IoT threats are associated with the web, application API, cloud, and mobile interfaces, and could significantly compromise the device and the associated data. Insufficient or

improper device authentication and authorization, as well as weak or no encryption, are all common issues related to IoT devices. Organizations can significantly minimize these vulnerabilities and IoT security risks by implementing privacy management solutions.

- As a result of increased cloud adoption, the organization's cloud security policy should be capable of protection against cloud security threats. Inappropriate cloud privacy security configuration is the main reason for enterprise cloud data breaches. Privacy management solutions address different issues such as accidental exposure of credentials, incident response, and data leakage over the cloud-based services, along with suggesting the remedial threat preventive actions on these respective issues.

Market Direction of Privacy Management Software

Privacy management software vendors are focusing on delivering simplified solutions that help organizations manage risks, create trust, and achieve excellence in an increasingly complex business landscape. Vendors will focus on increasing investments in product strategy, innovation, and professional services to better serve their customers. Additionally, in the years to come, organizations will focus on strengthening their efficiency by leveraging artificial intelligence (AI), machine learning (ML), and robotic process automation (RPA) to achieve advanced automation in their privacy programs.

In the coming years, it will become difficult for organizations to manage, supervise, and implement data protection regulations manually. Furthermore, constantly evolving, and demanding data privacy law obligations will eventually drive organizations to incorporate different privacy management solutions to maintain compliance with the ever-changing privacy management frameworks. The vendors of privacy management software are moving toward continuous developments in the areas of consent and privacy regulations globally. They are planning to provide global coverage for consent and privacy, regardless of the geographical region or sector, across the organization's privacy platform.

The companies are also focusing on data synchronization across internal systems to consistently honor customer preferences. These organizations are also planning

to offer consent and preference automation through robotic process automation for advanced workflows. Vendors are looking to provide a public suite of APIs that customers may use free of cost. With the help of these suites, organizations can allow their customers to view and update their consent and preference data.

Furthermore, vendors are planning to strengthen their integration capabilities to offer sensitive data intelligence through different connectors or integrators across their multi-cloud, SaaS, and on-premises privacy platforms. The vendors would continue to actively support data integration or data connectors with major cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Oracle Cloud Infrastructure (OCI) and focus on data extraction into their asset catalog.

Furthermore, the companies are also planning to offer a privacy platform that can discover, classify, and label multiple sensitive data items at scale in multi-cloud & self-managed and structured & unstructured data systems. The vendors are continuously focusing on automating privacy solutions by integrating privacy and regulatory intelligence, offering simplified legislative change solutions through their privacy management platform by broadening the scope of their existing control suggestion technology to suggest risks to the customers, and assisting stakeholders in implementing scalable privacy programs.

Quadrant Knowledge Solutions' SPARK Matrix: Privacy Management Software, 2022 research includes a detailed analysis of the global market regarding short-term and long-term growth opportunities, emerging technology trends, market trends, and future market outlook. The study provides a comprehensive market forecast analysis of the global market in various geographical regions and the overall market adoption rate as well. This research provides strategic information for technology vendors to better understand the existing market, support their growth strategies; and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

The research includes detailed competition analysis and vendor evaluation with the proprietary SPARK Matrix analysis. SPARK Matrix includes ranking and positioning of leading privacy management software vendors with a global impact. The SPARK Matrix includes the analysis of vendors, including Crownpeak, DataGrail, LogicGate, LogicManager, OneTrust, Poslovna inteligencija, Privacy Company, SAI Global, SAP, Securiti, Smart Global Governance, Syrenis, TrustArc, and WireWheel.

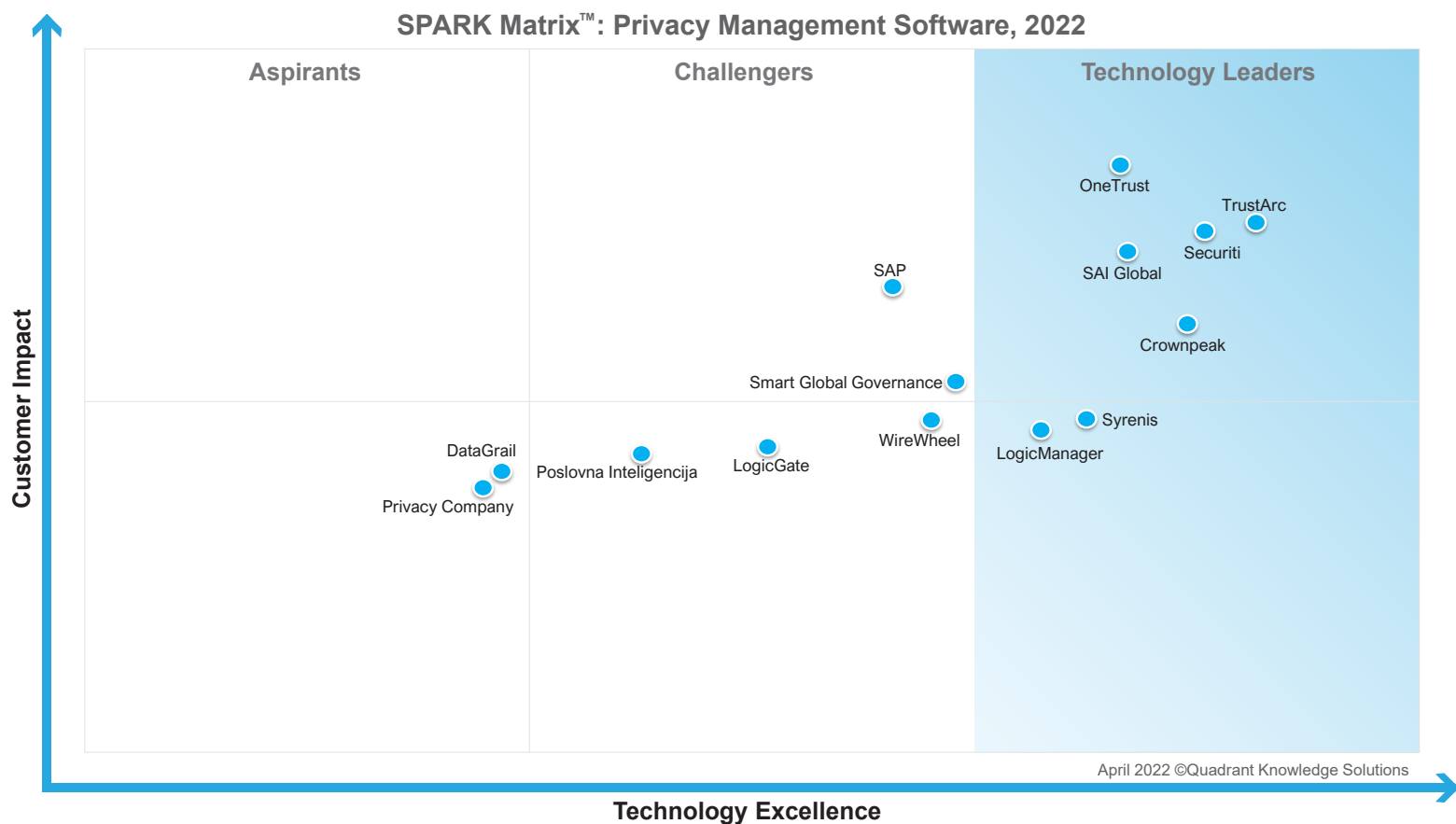
SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Privacy Management Software vendors by evaluating their product portfolio, market presence, and customer value proposition. Privacy Management Software market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants. It provides strategic insights on how each vendor ranks related to their competitors based on their respective technology excellence and customer impact parameters. The evaluation is based on primary research including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Privacy Management Software market.

Technology Excellence	Weightage	Customer Impact	Weightage
Sophistication of Technology	20%	Product Strategy & Performance	20%
Competitive Differentiation Strategy	20%	Market Presence	20%
Application Diversity	15%	Proven Record	15%
Scalability	15%	Ease of Deployment & Use	15%
Integration & Interoperability	15%	Customer Service Excellence	15%
Vision & Roadmap	15%	Unique Value Proposition	15%

According to the SPARK Matrix analysis of the global privacy management software market, “Syrenis, with a robust functional capability, has secured strong ratings across the performance parameters of technology excellence and customer impact and has been positioned amongst the technology leaders in the 2022 SPARK Matrix of the privacy management software market.”

Figure: 2022 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Privacy Management Software Market



Syrenis in the Privacy Management Software Market

Founded in 2000 and headquartered in Daresbury, Warrington, England, Syrenis is a provider of privacy management software. Cassie is the consent and preference management solution offered by Syrenis. Through customer service and continuous innovation, the company aims to deliver simple answers to challenging issues related to consent management and stakeholder involvement.

Cassie provides solutions for consent, compliance, and cookie management. Cassie offers various key features and functionalities, which include secure consent audit trails, central consent language repository, self-service preference centers (public portals), data harmonization engine, flexible integration function, sophisticated matching rule engine, data mapping (RoPA), and compliance management & reporting. The Cassie platform enables organizations to comply with global data compliance and regulatory laws. The platform also provides easy-to-manage consent, personal information, and marketing preferences from multiple sources through the data subject portal and assists organizations to develop their brand trust through transparency.

Cassie maintains an immutable record of every interaction an organization has with the data subject in a blockchain-style audit login through its secure consent audit trails capability. The platform has an administration portal that gathers all language consents centrally, which ensures that businesses can modify consent across various channels that are distributed along with their websites, applications, and systems from a single location. The company's flexible matching rule engine ensures that it can adapt to the client's business strategy for allocating consent. Cassie's self-service public portal enables organizations to allow their customers to view or update their consent and preferences. It also allows organizations to use the Cassie API to create their customized portals.

The platform's integration capabilities and real-time processing, coupled with its matching rule engine, facilitate data harmonization that provides businesses with the assurance that their PII and consent data is always in synchronization across all their systems. It provides scalability for enterprises that can accommodate hundreds of millions of data subjects and preferences. Moreover, data mapping enables records of how and where consent data and PII data flow through an organization. The compliance management and reporting capability of the

platform create dashboards with the help of different business intelligence (BI) and analytical tools such as TABLEAU, PowerBI, and Looker. Its flexible integration functionality makes the platform a flexible, secure, and scalable solution that easily integrates into any proprietary or third-party system.

Analyst Perspective

Following is the analysis of Syrenis' capabilities in the privacy management software market:

- Syrenis, through its flagship product, Cassie, enables organizations to centralize and integrate their consent and preference repositories into a single source. Through continuous innovation and customer support, Syrenis plans to offer simple and user-friendly solutions for complex issues related to consent management.
- Some of the key differentiators for Syrenis include a flexible data structure that can adapt to any organization's regulatory approach, data models, and integration requirements. It can support existing privacy regulations as well as new regulations that will emerge in the future. Additionally, Cassie offers API and a connector service module that synchronizes businesses' consent data throughout their systems, provides compatibility with any third-party, sales, and marketing platform or system an organization uses, and offers a matching rule engine that allows adaptations for consent allocations to the client's business. Furthermore, Cassie builds a data subject profile when the data subject first provides consent, and from that point, it decides its customer journey with the help of Just-In-Time workflows, which help handle a large number of outbound communications of data subjects across a variety of channels.
- Cassie's other differentiators include extended preferences to store data and real-time consent. With Cassie, clients can save as much custom data as they need in each consent record, which enables the development of a detailed consent and preference profile for data subjects that help manage complicated consent transactions and offer highly customized marketing and communications. API in real-time consent allows query handling of voluminous consent data in real-time.

- In terms of geographical presence, Syrenis is well-positioned in North America and Europe, followed by Canada and the Asia Pacific. Syrenis holds a strong customer base across a wide variety of industries, including retail & eCommerce, healthcare & life sciences, banking & financial services, government & public sector, education, and energy & utilities. It has ample scope to grow in the IT & telecommunications, manufacturing, media & entertainment, and travel & hospitality sectors.
- Some of the use cases of Syrenis's existing customer base include handling high volumes of customer consent data in the banking and financial services industry, collecting and processing sensitive consent data in the healthcare, life sciences, and retail industries, consent & preference management for the automotive industry, and compliance management for the media & entertainment industry.
- Syrenis's key challenges include the growing competition from emerging vendors with innovative technology offerings, as well as from small vendors. The company may focus on catering to small market businesses and supporting more use cases to accelerate its growth beyond the North American and European regions. However, with its sophisticated technology platform and comprehensive functional capabilities, Syrenis is well-positioned to expand its share in the global privacy management software market in the near future.
- Syrenis's strategic roadmap for the next 2 to 3 years centers around three key strategies. First, Syrenis is looking to build a trusting relationship with clients by enhancing the end-user experience and aims to offer cost-effective solutions. Second, regardless of the geographical region, the company focuses on continuous development in global consent and privacy regulations across all its platforms. And lastly, for smoother working of platforms, Syrenis is working on implementing AI for real-time decision-making across all platforms.