PRIVITAR

Data Sovereignty

Leveraging Data to Improve Organizational Performance is a Global Imperative

www.privitar.com

79% of executives agree that those who do not embrace big data will lose their competitive position and could face extinction, and 83% of executives reported they have pursued big data projects for a competitive edge, according to the Privitar Pulse Survey. Similarly, organizations that implement a data lake outperform similar companies:

> 9% higher organic revenue growth

> 4% better operating profit growth

> 45% decreased time to market

In today's global economy, data sources are distributed worldwide, and opportunities for growth and optimization are everywhere. Enterprises are creating analytics centers of expertise to maximize efficiencies, collaboration, accuracy and sophistication of models, and, ultimately, results. Often, maximizing these efficiencies means that these hubs are not colocated with every regional data center. Combining regional data can strengthen models and sharpen the insights and results they yield, but with this regional coordination comes increased complexity.

Protecting Sensitive Data is Critical to Movement Across Borders

There is a growing body of regulations that control what personal data can be moved across borders, including for data analysis. "Anonymization", the means of identifying an individual are sufficiently removed to protect their privacy, is critical in many of these regulations. The location of a data lake on a server in the EU may be compliant with GDPR regulations, for example, but sending the data for analysis outside of Europe without it being anonymized constitutes a "cross-border transfer" and is subject to strict parameters on where and what data can be sent. The US Privacy Shield Framework mandates that personal information about consumers must be treated as sensitive.

Opportunities for growth and optimization are everywhere

And China's government states that no data deemed important to the State can be sent outside the country without the express permission of the government; even then it must be carefully protected, a directive that has definite impact on global companies with multi-region clouds or regional data centers.

In order to protect the privacy of citizens and customers, these "cross-border transfers" are regulated by privacy laws and and organizational policies that limit what data can move where. These limitations can range from broad application, such as GDPR and the safe transfer of data throughout Europe, down to specific use cases, such as the HIPAA conduit rule regulating who has permission without a business agreement to temporarily transmit and store sensitive data. Failure to safeguard an individual's private information can result in significant fines or legal actions.

These complex regulations can present challenges for organizations looking to make the most of their data. Some organizations will simply keep data at a regional level, limiting the scope of their analyses, and the benefit to the organization and potentially even the customers themselves. But data leaders attack this challenge head-on. They build an understanding of the rules and regulations involving data transfers into and out of relevant regions. To build manual processes or custom solutions in-house is a huge task, which is why many enterprises are turning towards automated solutions that help them systematically manage what kind of sensitive data can be transferred, at what level of anonymity, and where.

Data Transfer Laws Require a Solution that Precisely Manages Privacy Across Borders

Clearly, there is no "one size fits all" for what levels of de-identification are required during cross-border transfers. This complexity can be a deterrent for enterprises wanting to use sensitive data, as they cannot scale a manual approach that ensures compliance with local regulations. To simultaneously optimize utility and maximize efficiency when keeping abreast of rules and regulations on data transfer, an automated and granular approach is the logical next step when managing the transfer of data across boundaries at scale.

Data leaders attack this challenge head-on

De-identification is significantly referenced in many different pieces of legislation. GDPR mandates data must be anonymized if it is involved in a transfer with a country whose privacy protections have not been approved. As of 2020 the approved list includes only 13 countries outside the EU and UK. Brazil's LGPD data protection law requires that personal data must be fully protected from any unauthorized access, and China requires protecting any data outside its borders. Increasingly, there are similarities that must be accounted for and correctly managed in order to ensure compliance with regulation while using data to the fullest extent:

- Anonymization. "Anonymizing" data to remove the ability to identify individuals allows more flexibility for organizations to send and receive data across borders. The degree of anonymization or the methods to do so may vary across legislation, so a range of options to best suit each use case is ideal.
- Fit for purpose. When it comes to moving data across borders, sensitivities run higher than normal. So, it is especially important to achieve data minimization and provision only the data required for each use case.
- Reversible de-identification. Any sensitive data that is relevant to data privacy laws must be protected, and in many cases, anonymized prior to transfer across borders. After analysis is done, however, it is often critical to re-identify individuals to take recommended individualized action, whether that is personalized marketing, next-best-action cross-selling, customer experience management or healthcare intervention. Such re-identification must be achieved in the original jurisdiction. The ability to anonymously evaluate the data and then re-identify it within safe borders is critical to actionable strategies.
- Tracking. Data must be tracked throughout its lifecycle, to ensure it is carefully monitored and used for the correct purpose, by the authorized people, at the appropriate time.

The Privitar Data Privacy Platform™: Maximizing the Safe Use of Sensitive Data Globally

The ability to analyze data across regions and jurisdictions gives organizations a competitive advantage and helps foster and solidify relationships with their customers. Cutting through the complexity of managing the transfer of data across borders, the Privitar Platform offers functionality that assists in automating, centralizing and precisely managing the different policy requirements that allow the best use of sensitive information:

- De-identification. Privitar provides the full range of techniques to anonymize data while still allowing evaluation of the datasets. De-identifying data will allow it to be anonymized to varying degrees according to the type of regulatory requirements the data is subject to when transmitted. Privitar supports redaction, reversible tokenization, generalization and perturbation among other techniques to achieve anonymization throughout the transfer and analysis process.
- Policy management. The Privitar Platform enables Privacy Policies to be defined centrally. Set policies by geographical region or by dataset to ensure the data is anonymized appropriately depending on the regulatory requirements. This design ensures Policies are applied consistently across environments, allowing enterprises to ensure uniform compliance with whatever sensitive data rules are specific to a region.
- Watermarks. Privitar Watermarks are unique technology that enable end-to-end traceability of sensitive data. Watermarks allow tracking and management of when a dataset was generated, who it was generated for, when it should be deleted and where it can be used.
- Re-identifying sensitive data. Privitar enables you to control reversibility so that you can re-identify anonymized data after analysis and take action on the insights gleaned from analysis.
- Separate roles. Providing separate roles for who can see and use data ensures even more control over processes related to data transfer and analysis. Key roles provided in the Platform are:
  - Administrator. Manage the environments included in the Platform.
  - Author. Create, edit and delete Privacy Policies, Schemas and safe datasets, which we call Protected Data Domains.™
  - Operator. Run jobs to de-identify data.
  - Investigator. The only role that can investigate and trace the origin of the data.
  - Unmasker. Run jobs to re-identify specified de-identified data that was originally defined by the Author to be reversible.

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136
US +1 857 347 4456
w: www.privitar.com

PRIVITAR

@PrivitarGlobal

www.privitar.com