Enabling Database Separation for Data Protection and Client Confidentiality in Group Companies

August 2024

Published by bilabl

Welcome to our August newsletter!

In this newsletter we will discuss how for many of the growth-biased members in the bilabl community, where group companies are operating across multiple offices, the composition of the digital suite is critical.

Within that technology ecosystem, maintaining robust data protection and ensuring client confidentiality become paramount issues. That requires the separation of databases between the operating entities, even if resources (human and otherwise) are ultimately being shared.

1. Enhanced Data Security

Separating databases for different offices within a group company significantly enhances data security. By isolating data, the bilabl community can prevent unauthorized access and minimize the risk of a data breach spreading across multiple offices. If one database is compromised, the isolation ensures that other databases remain secure, thus containing the potential damage.

Moreover, specific security measures can be tailored to the needs and threats of each office. For instance, offices in regions with higher cyber threat levels can implement stricter security protocols without affecting the operations of offices in more secure environments. This granularity in security management is only possible with a suite of digital tools that supports database separation, with bilabl operating as the engine that drives the workflows and data analytics.

2. Ensuring Client Confidentiality

Client confidentiality is a cornerstone of trust and reputation for any business, particularly in the realm of professional services. By segregating databases, group companies can ensure that sensitive client information is accessible only to the relevant office and authorized personnel. This approach reduces the risk of internal data leaks and ensures that client data is handled with the utmost care. The permissions matrix offered by bilabl is a further layer of security as projects and matters flow between team members, often in different jurisdictions. Database separation ensures that client data remains within the boundaries of the appropriate office. This is especially crucial for adhering to data protection laws that mandate data localization and restrict cross-border data flow.

3. Regulatory Compliance

Compliance with data protection regulations such as the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA) in the United States, and other regional data protection laws is incredibly important for all professional service firms, whether corporate services or pure legal. These regulations require stringent measures from the bilabl community to protect personal data and ensure its confidentiality.

In our experience, a suite of digital tools that supports database separation allows group companies to comply with these regulations far more effectively. For instance, under the GDPR, personal data must be protected against unauthorized access and data breaches. By segregating databases, companies can implement compliance measures tailored to each jurisdiction, ensuring that local data protection laws are met without impacting global operations.

4. Operational Efficiency and Flexibility

Database separation also enhances operational efficiency and flexibility. Different offices in the bilabl community can operate independently, with databases tailored to their specific needs and workflows. This autonomy allows for faster decision-making, more agile responses to local market conditions and client requirements, better resource allocation and, ultimately, higher growth in revenues and profitability.

Furthermore, database separation simplifies the management of data lifecycles, backups, and recovery processes. Each office can develop and maintain its database management policies, ensuring that they align with local best practices and regulatory requirements. This decentralized approach reduces the complexity of managing a unified database system and enhances overall operational efficiency.

5. Risk Mitigation and Business Continuity

In the event of a cyberattack, natural disaster, or any other disruptive event, having separated databases can significantly mitigate risks and enhance business continuity. A breach or failure in one office's database does not compromise the entire company's data infrastructure. This isolation allows unaffected offices to continue operations, maintaining service delivery to clients whilst providing support to the affected office and its suite of clients.

Moreover, the ability to implement customized disaster recovery plans for each office ensures that data can be quickly restored and business operations resumed with minimal downtime. This resilience is crucial for maintaining client trust and protecting the company's reputation in the face of unforeseen challenges.

6. Possible negative side-effects of data separation

However, with data separation, it will be more difficult to perform data processes on a multiple-tenant level. So, this will for example impact the possibility to perform a conflict check. Furthermore, if you work with multiple entities within your group but there is no connection between each entity, the same client may be added under different names under the various entities. To address this issue, you should create a master database for shared data and each office can access and synchronize the information. For compliance and security reasons, the private data will be held at tenant level only.

Conclusion

Putting all of this feedback together, it is clear that curating the appropriate composition within a suite of digital tools is essential for any high growth, professional services firm. At the same time, one of the fundamental elements of this process should be the facilitation of database separation across multiple offices. With bilabl as part of this suite, group companies within the community are able to enhance data protection, ensure client confidentiality and comply with regulatory requirements.

In doing so, this strategic approach not only bolsters security but also provides operational flexibility and risk mitigation. Data protection has to be paramount to every firm and database separation stands out as a vital practice for safeguarding sensitive information. To find out how bilabl features as a key part of the solution contact us here for a demo.

Profits will grow as a result. We have the data to back this up! Implement strong data governance policies to ensure data integrity and invest in the IT capabilities to execute this.