“One to serve them all”

A case for centralising data hosting services worldwide from a functional and legal point of view

Drs. Paul Kromhout RE CISA, drs. Jeroen Tegelaar and Maurice Koetsier MSc CIPM

Many companies worldwide are in the process of harmonising their IT system landscapes and centralising their hosting of several types of business and personal data across their local subsidiaries worldwide. This is not an easy feat to accomplish: besides the technical and organisational challenges associated with such a project, a variety of regulatory requirements and conditions are applicable to successfully centralise IT and data hosting and at the same time be compliant to (local) rules and regulations. This article presents an overview of the conditions companies will need to meet when they want to centralise and modernise their IT system landscape on a world-wide scale. It presents the case of a German company which had to deal with the challenges of centralisation from a regulatory and functional perspective and the process of how to achieve this. It also delivers a proven methodology and recommendations for readers who are searching for guidance and lessons learned when dealing with a project of the same nature and complexity.

Drs. P.N.M. Kromhout RE CISA
is a senior manager at KPMG IT Advisory.
kromhout.paul@kpmg.nl

Drs. J.A.C. Tegelaar
is a senior manager at KPMG IT Advisory.
tegelaar.jeroen@kpmg.nl

H.M. Koetsier MSc CIPM
is a senior consultant at KPMG IT Advisory.
koetsier.maurice@kpmg.nl

Introduction

Many companies are consolidating and/or improving their IT landscape after years of relative neglect following the financial crisis of the previous years. As such, they are in the process of harmonising their system landscape across their subsidiaries. In line with this harmonisation, centralisation of IT management and hosting (at one or a limited number of locations) also becomes more apparent.

Besides practical questions with respect to technical and organisational issues, companies also need to take into account how to respect the vast amount of existing local laws and regulations. No country in the world (not even in Europe) applies exactly the same laws and regulations with respect to, for example, data storage, data retention and data (information) security.

The primary question that every company needs to answer when they are considering harmonisation is “Are you allowed to host the data in another country?” and if “Yes, but ...”, then which criteria apply. These criteria can be related to some of the following questions:

- If the company wants to transfer data across borders, what are the transfer restrictions?
- Which retention periods apply to different types of information/documents?
- In which format can information be stored?
- Under what conditions is it allowed to host sensitive data?
- How quickly should you be able to respond to data requests, either by the authorities or third parties?

The case for harmonisation

The answers to these questions differ per company and the sector they are working in. However, there are lessons to be learned that apply to any company in any sector. This is best demonstrated by describing the following case:

“An International Lease company, with corporate sites in over twenty different countries located in Europe, North America, South America as well as Asia, had to identify which conditions for the individual countries needed to

be met in order to make centralised hosting of data possible. This question was related to the implementation of the new IT Strategy and subsequently the alignment of this strategy with the objectives of the business. The main goal was to harmonise the business processes and the underlying operating model and to harmonise the IT platform and landscape."

Before the project started, the business activities were supported by eleven different contract management systems across all the countries. This had the following consequences:

1. Relations had to be maintained with more than eleven different software suppliers. The operating systems running on those systems differed between the countries and were partly carried out by external local service providers.
2. The ability to integrate the various country platforms into group core systems and processes is limited, which becomes more and more relevant from a group reporting perspective.
3. Apart from the reporting aspects, time consuming roll-outs of new product introductions or global initiatives make the company less competitive and if system changes are needed, a high dependency on local key IT personnel will continue to exist.

The project's objective was to replace the eleven applications with one standard application with limited localisation and to standardise the way of working worldwide to improve efficiency and at the same time reduce the IT costs of maintenance.

The first steps for improvement and the first lessons learned

After completion of the software selection procedure for one new contract management system a Global System Template was created for managing the leasing business as well as the financial accounting process. Subsequently, in a similar selection procedure, an IT service provider was selected to provide the data hosting services necessary to make the new IT system work in day-to-day operations. Initially, this provider was also given the following tasks for the countries within the scope of the project:

1. Identify the local restrictions (rules & regulations) that could restrict the possibility of centralising the systems in a limited number of regional data centres.
2. Provide an answer to the question of whether there were stricter laws/regulations for application delivery than in Germany and if there were local requirements that were blocking the centralisation of the application.
3. Provide insight into regulatory or legal requirements that would delay or block a local entity from going live with the new system on a functional level.

This proved to be too much of a challenge for both customer and provider. Both parties formulated their initial answers to these three questions from such an operational and IT security perspective that it resulted in a list of requirements that differed vastly for each country and could be interpreted differently for each subsidiary. The second challenge was that the IT service provider was not (yet) based in all eleven countries within the scope of the project and could therefore not identify all regulatory or legal requirements that would delay or block a local entity from going live. They simply lacked the resources and knowledge to do so.

Adjusting the approach

The project looked for a party that could provide support with answering the above questions. As such the project team was asked to support both the customer and the provider in this matter. The three questions remained unchanged, but to increase the chances of success, the scope of the activities was limited to the core processes of the company and the actual roll-out of the IT system with a focus on:

- the functional requirements of the system;
- centralising data/systems in a data centre;
- operating these systems in a data centre.

The regulations examined were limited to regulations that directly stated a requirement for central hosting (such as central banking regulations, banking act, tax law) and only at a high level. Regarding the requirements the following approach was used:

1. Identification of requirements was performed based on the available documentation of the customer, legal sources, retention guides and previous research papers of earlier engagements in the field of data retention, data privacy and data transfers.
2. Validation of requirements for the 23 countries was performed by local privacy and legal experts from the project team's global network. An overview of the

When requirements are still missing, a reference can be made to a related standard or to the requirements of a directly neighbouring country with similar laws and regulations

activities performed is provided below and the most important steps are further elaborated upon.

The results were used to provide insight to determine the impact of possible blocking issues per country and the identification of mitigating measures per issue. Because the roll-out of the system was planned in five waves of clustered groups of countries, the research was planned accordingly.

Consolidating a proven methodology

Based on experience in previous projects, the following methodology was set-up and validated with all stakeholders. The different steps of the methodology are as follows:

Step 1: Set-up/actualisation of a survey

To correctly identify and include all relevant functional and legal requirements a survey on transfer restrictions, privacy issues, format restrictions and retention tables needs to be developed through a series of stages. The survey can be developed by using available knowledge, similar queries and customer specific queries. The customer should review and provide feedback to customise and align the questionnaire to the customer's specific situation. In this case, input from the earlier survey of the already mentioned IT service provider was also used to complete the list of questions.

With the questionnaire as a blueprint, the analysis of the laws and regulations focused on the identification of those regulations that directly address the rules regarding the centralisation of hosting and possible restrictions.

Step 2: Identification and categorisation of requirements per wave

During the identification and categorisation phase of the project, good practices should be used to identify the relevant requirements for all countries per wave and to judge if those requirements are consistent with each other by a core team and specialists within the project. The respective team members should complement the requirements for each country, validate the lists and provide recommendations for hosting requirements. When requirements are still missing, a reference can be made to a related standard (such as ISO27002 on Information Security) or to the requirement of a directly neighbouring country with similar laws and regulations. See Table 1 for an example specifically focused on data retention.

In this case, after the delivery of the requirements of the first wave, specialists from India were included in the core team to speed up the progress to accommodate the planning of the customer.

In parallel, local experts were identified and contacted to validate the identified requirements for the corresponding 23 countries.

Step 3: Provide (re-)usable insights

After validation of the requirements, the next step is to gain a solid understanding of the results and apply these to the objectives of the customer. Using the recommendations of the specialist international network the core team should be able to interpret the legal requirements in such a way that country specifics are taken into consideration, without losing the overall view on all countries.

By gathering information on hosting requirements and conversing with the customer the project team is able to formulate recommendations on how to proceed with the harmonisation of the systems on a functional level and centralisation of hosting.

For this project, Germany was used as a starting point for developing functional requirements as it deals with the most strict requirements (from a legal perspective) and main centralisation was deemed to be in Germany. German locals took a leading role in this process based on their experience with specific German requirements and with the customer. The results of the requirements on hosting were subsequently clustered in a set of conditions that apply in general to all the countries within the scope of the project (see Table 2).

Analysing the results and providing recommendations

The results of the identification of requirements show a lot of similarities of general conditions for the different countries worldwide. For Russia and Turkey it was not allowed to store data outside the country (see Figure 1). For the other countries it was allowed to store data outside the country but under the condition that the country in which information is stored guarantees an adequate level of protection.

ERP process	Document Categories	Starting Point Retention Period	Minimum Required Retention Period	Underlying Legal Requirements	Exception
Record-to-report	General ledger, accounts payables, account receivables, asset accounting, sub-ledgers, tax, etc.	Posting date subsequently start of FY	10Y	Art. L123-22 paragraph 2 French Commercial Code	Bank deposits: 30 years (L221-5)
(Indirect) Tax	VAT	The end of the relevant FY	3Y	Article L176 LPF (FrenchTax ProcedureHandbook)	None
Plan-to-Budget	Cost element accounting, cost centre accounting, internalorders, activity-based costing, product cost controlling, profitability analysis, profit centre accounting.	Posting date subsequently startof FY	10Y	Art. L123-22 paragraph 2 French Commercial Code	None
Cash & Treasury Management Fixed Assets	Treasury and risk management, cash and liquidity management, in-house cash, mortgage accounting, real estate accounting, investment accounting, etc.	Posting date subsequently start of FY	10Y	Art. L123-22 paragraph 2 French Commercial Code	None
Prospect-to-Order Order-to-Cash	Sales, deliveries, pricing conditions, billing, shipping, transportation, customer service, credit and risk management, customer master data, agreements, etc.	Posting date subsequently start of FY	10Y	Art. L123-22 paragraph 2 French Commercial Code	None
Source-to-Contract Purchase-to-Pay Receive-to-Leave Material-to-Product	Purchasing, inventory management, evaluation, orders, contracts, purchase requisitions, vendor master data, vendor conditions.	Posting date subsequently start of FY	10Y	Art. L123-22 paragraph 2 French Commercial Code	None
Hire-to-Retire	Recruitment, personnel management, payroll, travel and expenses. time management, benefit Management, training and event management etc.	Posting date subsequently start of FY	HR: 5Y Recruitment: 2Y	HR: Art. L3243-4 French Labour Code Recruitment: CNIL Recommendation n° 02-017	None
Other	Additional data archiving requirements which are not falling under the above listed categories.	Posting date subsequently start of FY	6Y	Tax instruction 2006	None
* Format of back-up	In principle, the company books and records may be created and retained in electronic format. The requirement that the company's rights and obligations must be able to be presented at any time entails that the authenticity and integrity of the electronic records should be adequately ensured & electronic records should be accessible during their retention period.				
** Response time for accessing the data	The electronic records should be made legible within a reasonable time frame.				
*** Data distribution / storage location	Electronic copies may be stored at the premises of the company or by a third party. The country of storage needs not be located within the EEA provided that adequate levels of protection are ensured for such data, in compliance with EC standards. Electronic invoices must be stored in France, in another EU member state or in a country bound by a mutual administrative assistance treaty with France.				

Table 1. **Sample of list of requirements for data retention.**

The US was no longer deemed adequate by the European Court of Justice, as data transfers between the EU and US under Safe Harbour were ruled invalid on 6 October 2015, so additional mitigating measures are necessary.

Based on these results the following recommendations are to be taken into account:

- Notify or obtain approval from the authorities for the hosting data. Prior to hosting data outside the particular countries it is advised to notify or obtain approval from the particular authorities. For the countries in which data should be available on-site for inspection by the authorities it is recommended to periodically send copies of the database to that country (or have online access to this data).
- Store all physical documents locally and ensure the possibility of a timely response of delivering digital data. To ensure timely response to inquiries from the authorities for inspection of the data or documents we recommend, for all of the countries in which a local subsidiary is present, to store and archive physical documents locally. We also recommend to ensure (online) timely access to systems and have a policy or procedure in place in case data access requests occur (either by government or data subject access requests from individuals with regard to personal data).
- Make clear agreements with third parties when processing personal data. When personal data is processed or transferred to a third party it is advised to take preventive measures. An example of such a measure is a formalised data processing agreement with the third party to have

Conditions that apply to data hosting requirements	
Notification of or approval needed from the Authorities prior to hosting	Notification: in Hungary, Poland, Sweden Approval needed: in Portugal, Spain, Canada, France, China, Luxembourg and Italy.
Copy of database sent to country of origin	Requirement for: Romania, Sweden, Ireland, UK, Luxembourg, Italy and Brazil
Physical documents (invoices, P/L, financial statements, etc.) should be stored in country of origin	Requirement for: Portugal, Spain, Poland, Romania, Sweden, Ireland, UK, Luxembourg and Italy
Requirements should be equal to / exceed those of the country of origin when compared to a central location	Requirement for almost all countries worldwide, extra reporting needed on software for China
Retention period of accounting / financial data	For most countries 7 to 10 years
Data should be available or accessible to the Authorities in a reasonable timeframe (includes archiving)	Requirement for all countries, required time limit for delivery from a minimum of 8 hours (banking data Brazil) to 'within 15 days' (Luxembourg)
Test data must be anonymised	For all countries test data should be secured properly, for some consent of the owner is needed (Canada
Insight required into data flows to ensure compliance on data transfer	This is a requirement for most countries worldwide
Data in decommissioned systems remains legible for duration of the retention period (data integrity) in case of partial data migration or archiving	This is a requirement for most countries worldwide
Additional requirements apply when processing personal data in another country	This is a requirement for most countries worldwide
Data processing should be formalised via agreements when using third parties	Requirement for: US and Brazil

Table 2. **Summary of conditions and some examples of conditions per country.**

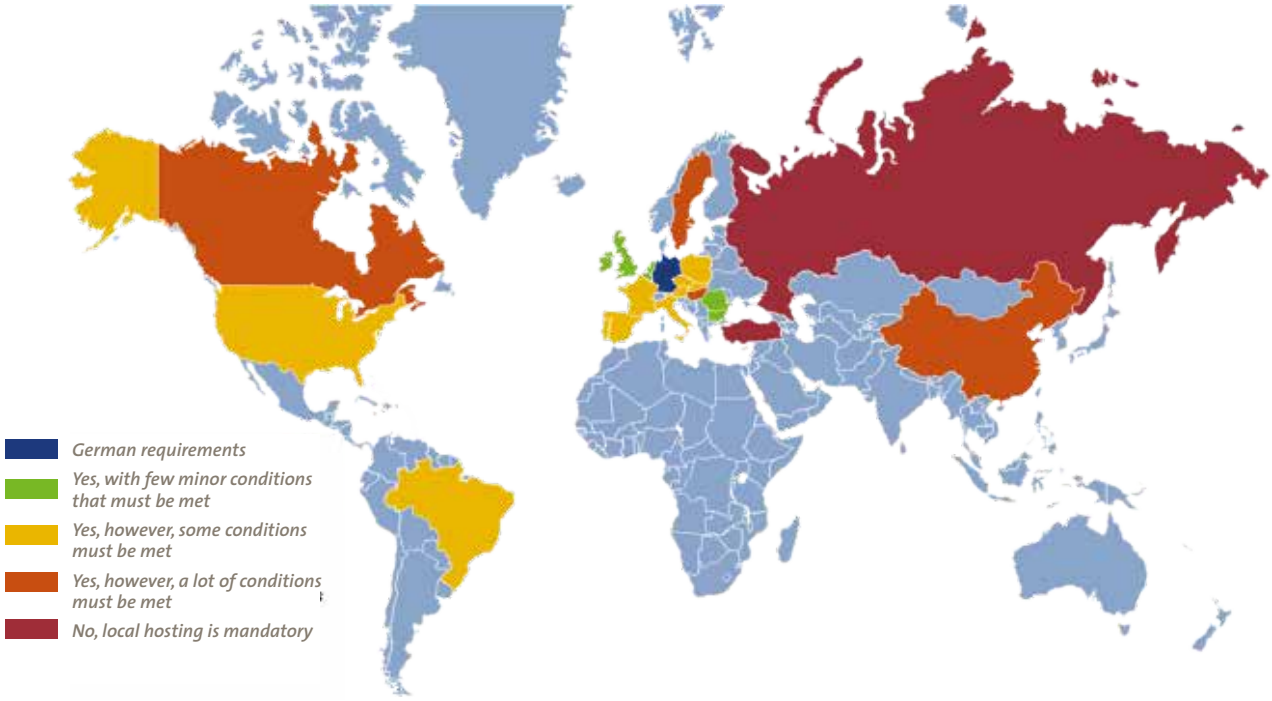

Figure 1. **Overview of conditions per country.**

them adhere to a company's security and privacy policy. To comply with privacy laws and regulatory requirements it is further advised to identify and map the current data flows to get insight into international transfers and whether data is transferred to countries that do not provide an adequate level of protection.
For these particular countries companies should apply alternative measures to ensure compliance (i.e. model contract clauses and approval of the European Commission, binding corporate rules).

- Develop and implement a security and privacy baseline to ensure compliance with local requirements. We recommend to develop and implement an organisational security and privacy baseline based on 'good practices' (e.g. ISO27002, Data Protection Acts, etc.) to comply with local regulatory requirements. This baseline should address anonymisation of test data and security of test environments to prevent data breaches from happening. The baseline should also include upcoming changes on EU privacy law.
- Develop a records management[1] policy with a records retention schedule. We recommend to develop/extend the records management policy for the countries in which Deutsche Leasing operates ([Tege12]). This policy should include a records retention schedule for different data categories and different document types (to include unstructured data such as documents on file shares). A record management policy should ensure integrity and authenticity of stored/archived records as elaborated upon in 'good practices' in the market (e.g. ISO15489). A records management policy should also address the topic of data migrations.
In the case of partial data migrations at the company, data of decommissioned systems should remain legible for the retention period, meaning that this data and archived data should be accessible and readable even if there is no platform to mount and read the data. This implies that data should be stored in a sustainable format.

Conclusions

What are the lessons learned from this project?

First of all, stick to what you know and be honest about what you do not know. The combined efforts of the company and the IT service provider were to be recommended, but to provide for the necessary world-wide insight into regulations on data you need to have the experience, expertise and the capacity to deliver.

Secondly, focus on similarities between countries and not on the limitations. Of course when investigating over twenty countries on regulations and guidelines, the result will always be over twenty different sets of requirements. But, in all cases some generic conditions can always be identified that should be taken into account when moving systems and data across countries in order to be able to centralise hosting. In essence, there are more possibilities than it seems at a first glance. It does help if the main hosting country is one of the countries with the strictest rules. This simplifies the condition that the rules and regulations in the hosting country should have at least the minimum level of the originating country in order to comply with rules and regulations of these countries.

1 Records management is mostly focused on archiving unstructured data and related metadata. For a detailed approach on how to set-up and implement data archiving for structured data, see [Tege12].

In general, centralised hosting is possible within Europe, leaving out the odd ones such as Russia and Turkey.

Thirdly, regulations always need to be interpreted. A judge is not a machine, so a company always needs to explain how they deal with compliance to certain regulations. It is interesting to see that companies tend to forget that they need to allocate time and resources beforehand to do exactly that interpretation. The reason for this could be the general misconception that regulations are absolute and complete and therefore they need to be obeyed strictly. In dealing with requirements for 24 countries a company will soon enough realise that this is just not feasible. Having someone on your team who can translate requirements to actions in your daily business and who can provide an overview of the similarities between jurisdictions is not only recommended, but even a critical precondition for success.

Finally, please note that laws and regulations may sometimes already be outdated during the investigation as new rules are being implemented all the time or existing rules (such as data transfers to the US) might be part of political discussions. For this reason you always need to timestamp your assessment when dealing with regulatory supervisory bodies and implement a maintenance process of actualising your earlier results on a structural base.

Reference

[Tege12] J.A.C. Tegelaar, P. Kuiters and J.M.B. Geurtsen, *Data archiving in a digital world. Roadmap to archiving structured data*, Compact 2012/2.

About the authors

Drs. P.N.M. Kromhout RE CISA has over 16 years' experience at KPMG and works within IT Advisory Risk Consulting Financial Services. Activities include performing audits on IT management, system audits and data analytics as part of financial statement audits and/or advisory assignments such as system selections, system implementations, data migration and process mining. He works within the financial services sector, predominately at large banks and leasing companies.

Drs. J.A.C. Tegelaar is a senior manager of KPMG's Dutch IT Advisory practice and a core member of the Enterprise Data Management team and has over 15 years of industry and advisory services experience. He has a background in Data Governance, Data Quality, Data Migration, Data Privacy and Enterprise Content Management. A lot of his engagements are about supporting companies in identifying and translating regulatory requirements on data to practical action for global business.

H.M. Koetsier MSc CIPM is a senior consultant in the Cyber team within KPMG's Dutch IT Advisory practice. He has over 4 years of experience in various sectors and advises international organisations in the field of data privacy and cyber security. He is a member of the NOREA Privacy working group and one of the driving forces of the Dutch Privacy Team.