No stone unturned

Forensic Technology
Data Remediation Services

kpmg.com/uk
Contents

No stone unturned 3
Communication holds the key 5
Streamline the process 8
Identify the data 12
Technology solutions in deals and transactions 13
Maximise value, minimise risk

When companies sell a business, intellectual property (IP) and commercially sensitive information (CSI) are a significant part of the value. Failure to separate data could result in important information passing to the acquirer or leaving the sold business without information needed for it to function. Effective data separation is often a regulatory requirement: getting it wrong risks the deal being blocked by the regulator, delays and legal or regulatory action after completion if mistakes are made.

Forward-thinking companies are addressing these risks at board level when divestments are planned. To ensure effective separation of data on completion requires planning, a clear strategy and the involvement of internal and external stakeholders. Only on implementation does the scale of the project become clear.

The complexity and sheer volume of data involved can be daunting but with careful planning and a proven workflow the process can be streamlined and managed to completion. Doing so ensures a proportionate response that reduces cost and disruption and protects business value. Failing to do so risks a costly, over-engineered response or leakage of data when remediation options are not acted on.

Companies are increasingly putting their data in order before any decision to sell a business.
Doing so makes divestments easier to manage and can increase the value of a business to be sold by assuring the buyer they will receive particular data in a good state.

Pre-emptively addressing data by adopting an information governance framework helps companies cope with data overload by establishing guiding principles and upholding categorisation and retention policies.

Getting data separation right leads to:

— **Security of valuable business information**

— **Minimal cost and disruption**

— **Completion of the transaction by deadline to the regulator’s satisfaction**

— **Reduced legal and regulatory risk**

KPMG’s experienced, established team has worked on the successful completion of complex divestments linked to some of the world’s biggest deals. Our workflows, procedures and technology have been tested in the market and are ready to be deployed to get the deal done.
Communication holds the key

KPMG can help you identify CSI and define which data should be removed from the business and which should stay. But data remediation is not simply a technical process. It involves people with their own requirements, business practices and pressures on time and resources.

Too often data is not prioritised early enough in transaction planning. We recommend creating a separate data team from the outset. This team should have a clear remit to work closely with IT, legal, marketing and other teams. Collaboration, senior stakeholder involvement and clear lines of communication should be built from the start.
Key priorities

- Bring together business functions, HR, legal and IT to define a standardised approach that saves time and cost.

- Engage with the business early to understand data sources, dependencies, applications and business practices.

- Understand the flow of data within the business and when it sits with third parties or other business functions within the company.

- Consult with regulators and legal specialists to build the right mitigation into data remediation methodologies to ensure the programme is compliant.

- Put in place structured workflows to agree the data identification process with the business with regular staging points to satisfy the regulator or the buyer that the workflow is appropriate.

KPMG can advise on and help establish these communication flows. We can also educate and provide know-how to the in-house IT team through a joint working relationship. If IT infrastructure is managed by a third party, KPMG works directly with them and their software to make the process as seamless as possible.
Streamline the process

Once a team is in place and lines of communication are established, you need a robust, structured plan to identify and transfer the IP assets. With data sitting in multiple locations – from strategically important plans and presentations to millions of emails – the task can be daunting. With careful planning the process can be streamlined using proven methods, an innovative approach and specialist technology.

The aim should be a smooth, cost-effective process that minimises impact on the business and creates an auditable, accountable process that has the confidence of all stakeholders.

KPMG’s team can design and implement a plan tailored to your business and the requirements of the transaction.
Key elements are

A set of guiding principles for classifying data for retention and divestment. The principles should be ratified by legal and, where appropriate, the board to ensure stakeholders understand the requirements and can separate data using their specific business knowledge.

Structured workflows to agree the data identification process with the business with regular staging points to satisfy regulators and/or the buyer that the workflow is appropriate. These workflows include:

— Workshops with application owners to identify the data that is most relevant to their department and function

— Questionnaires and meetings with creators and users of the material

— A book of evidence and a statement of fact that can be used to reassure and respond to regulators and other external stakeholders

— Technology solutions that automate the classification, migration and cleansing of data using a rules-based approach to classify documents based on content such as keywords and phrases, concepts and themes, date ranges and transaction numbers. This approach allows large tranches of data to be dealt with quickly, in a uniform manner and with minimal business impact
**Audit and accountability** to provide clarity on where different categories of data reside after separation:

— **Escrow**: documents containing data that may be needed later and that does not exist elsewhere in the business may be placed in escrow for access at a later date

— **Mixed documents**: where a document contains CSI relevant to the divested business and separate CSI related to the retained business, redacted versions are created for each business

— **Ringfencing**: documents required for audit or tax purposes or that may be called on after completion will be ring-fenced

KPMG’s established team has the expertise to manage the process based on experience gained working on complex transactions linked to some of the world’s biggest deals.
Identify the data

Business data sits in multiple formats and locations. Sources include mailboxes and emails, shared or collaborative mailboxes, data from SharePoint, servers and shared drives. Data relevant to a divestment can be divided into three categories:

**Commercially sensitive information**
- Cost/price information such as pricing per customer, suppliers’ pricing, plans and budgets
- Operational performance data providing insights into production volumes, capacity/utilisation data on matters such as manufacturing KPIs and supply chain planning
- Plans, strategies and other specific data
- Innovation projects specific to the divested business
- Governance reports on subjects such as risk, audit, fraud and penetration test results
- External data – only non-syndicated research

**CSI to be removed from the divested business**
- Best practices, ways of working and know-how
- Efficiency improvement projects or other capital projects to improve performance
- Innovation projects not yet implemented
- Long-term strategies not related to the divested business covering subjects such as procurement, supply chain, commercial categories

**Exceptions that may be retained by both parties**
- Information more than three years old at the date of separation
- Plans and budgets for the period
- Data required for financial, audit and tax purposes
- External data – syndicated research
- Information needed for continuing operation of the divested business including technical/packaging and engineering standards, marketing and finance methods
- Projects that have been communicated and are part of the divested business’s development plans
Technology solutions in deals and transactions

The brand sell-off

As part of a $100 billion merger between two well-known household brands, the European Commission and US Department of Justice ordered the divestment of certain brands, owned by our client, before allowing the deal to complete.

More than 60,000 employees were involved in the manufacturing and distribution of these brands in over 40 regions.

The volume of data was over 450TB of unstructured data (including emails and edocs) and more than 120 applications. KPMG identified more than 8,000 employees who potentially had CSI and were in scope for the remediation process.

Completion of the deal required this CSI to be hived out for handover to the purchasers and for the relevant regulators to receive evidence-based reassurance.
The approach

KPMG deployed a specialist data remediation team to work with the client to identify and scope potential data sources.

Using technology-driven solutions, interviews and online questionnaires, KPMG identified and defined the CSI for each business area to understand the movement of this data within the business. The workflow generated a full audit trail of the data sources and associated business decisions.

Once instances of CSI were identified, KPMG deployed specialist technology to identify further instances of this CSI and map where these items were disseminated throughout the business.

More than 500 million files were scanned for CSI and a remediation programme was put in place for hiving out of over 0.5 million instances of CSI across SharePoint, MS Exchange, user machines and fileservers without impacting business as usual.

The results

The client met the requirements of the European Commission and Department of Justice on time and on budget. The deal was completed without delay and avoided multi-million pound penalties.

KPMG provided a detailed audit trail and book of evidence to the client on completion to allow it to respond to regulators and purchasing third parties at a later date, if required.

All parties were confident that the right data was handed over with the divested brands and our client was cleansed of any relevant CSI while ensuring that business as usual was not affected throughout.

KPMG put in place workflows to ensure the management of any additional data identified after change of control as part of its ongoing risk mitigation programme.
The legal dispute

A long-running IP dispute with a joint venture life science partner settled after eight years of litigation.

The settlement agreement involved the forensic identification, separation and ultimately the remediation of IP from client IT systems.

Data volumes collected exceeded 60TB, covering 340 employees’ IT equipment and 16 application platforms.

IP that was identified and agreed as relevant by both parties was deleted from client systems.

Given the volume of data and court-ordered timelines, manual identification and deletion were impossible.
The approach

KPMG built out a full data landscape model and worked with both parties to devise and agree a methodology to identify relevant IP. This allowed early removal of non-relevant and non-user generated files before hosting and review to drive down costs.

The KPMG team integrated customised technology into the client IT environment to support the collection, processing and identification of data across eight regions including US, South Korea, China, UK, France, Singapore, Brazil and Belgium.

Over 57 million individual documents were processed and searched as part of the agreed workflow.

KPMG created a bespoke workflow to automate the collection and deletion of relevant material from client systems with minimum impact on business activities.

The results

The client achieved the court-mandated deadline, avoiding potential additional legal action and financial sanctions.

The result was achieved without any additional IT headcount.

The opposing party accepted the implementation of KPMG’s workflow.

Automated review technology and processing workflow tagged an additional 750,000 items, representing multimillion-euro cost savings.
Divesting a division

The challenge

As part of an £11 billion divestment programme of a major energy distributor, our client, under mandate from the UK regulator, had to demonstrate the logical separation of data between two elements of its business.

The client had to show that both companies could not access the same data locations across its entire infrastructure, including network folders and Microsoft SharePoint and Exchange environments. Additionally, over 300 structured data applications required testing, remediation and validation of access controls.

More than 7,000 employees were in scope with a requirement to validate that their access controls adhered to the regulatory requirements for separation.

KPMG was also required to educate employees on how to manage CSI.
The approach

KPMG’s Forensic Technology team designed and implemented a tailored approach to interrogate and address each of the challenges faced by the client.

KPMG worked with the client’s HR and legal functions to develop an education programme on personal data management that was disseminated to all in-scope client employees.

We developed and deployed customised scripts to retrieve access controls on each system for each user. Over 2.5 million structured data locations were analysed to identify access conflicts between both businesses.

Workshops were held with key stakeholders to address conflicted access controls. Remediation plans were developed so that business as usual and data dependencies were not affected.

KPMG worked with the client’s business application experts to design remediation plans for structured data applications where conflicting access controls were identified.

The results

By demonstrating logical separation of data within the relevant business elements, the client avoided significant regulatory sanctions. Where risk issues were identified, a remediation plan was implemented.

KPMG provided the client with a detailed audit trail and book of evidence on completion to allow it to respond to the regulator and purchasing third parties.

The buyer adopted KPMG’s workflow and processes to ensure data was managed effectively on the opposing side.

KPMG provided the client with insights and proposed areas for improvement of data management procedures and information governance.

Workflows were developed and implemented within the business to address management of CSI up to and after point of sale.