www.pwc.ch

In the era of data protection, less (data) is more

Strategies for analysing your IT landscape and building state-of-the-art records management in order to balance the conundrum posed by regulatory requirements in a world where information is gold

pwc

Contents

1 Executive summary 4

2 Regulatory background 6

2.1 Data protection in the EU – GDPR 6

2.2 Data protection in Switzerland – FADP 8

2.3 Regulations for financial services companies in Germany and the Netherlands 8

3 Implementing state-of-the-art data minimisation capabilities as part of data and records management 10

3.1 Defining the scope of your data and records management initiative 11

3.2 Risk-based approach to implementing data minimisation capabilities 11

4 Typical challenges observed in the journey to better data and records management 15

4.1 Insufficient ownership of the IT landscape 12

4.2 Dependencies on third-party providers 14

4.3 Processing of physical data 14

4.4 Processing of unstructured data 14

4.5 Decommissioned applications 14

5 Call for action 15

5.1 Decision tree: Where do you stand on your data and records management journey? 15

5.2 How can PwC help you? 16

1 Executive summary

Ever-increasing amounts of data are being collected, processed and stored every day. Leading big data companies such as Google, Amazon or Facebook play a key role in shaping the era of data and have contributed to spreading what is now a universally recognised dogma: Data is gold.

When properly processed and analysed, data can provide valuable information that a company can use to gain competitive advantage. This explains why companies all over the world years ago started collecting data from any possible source. And there is a lot of data out there: in 2018, 2.5 quintillion bytes of data where created every single day.[1]

However, due to the enforcement of stricter data compliance regulations around the globe, the idea of "the more data, the better" is slowly changing. Today, the tendency for many companies is shifting from collecting large amounts of data to a more selective approach to data collection. Due to the risk of fines relating to data protection throughout the world –especially in Europe with GDPR – companies need to understand what data they are holding, how they are processing it and for which purposes. Since data protection regulations require that data is only processed and held as needed for its original purpose (unless otherwise communicated to the data subject), from a compliance perspective it is essential to know the answer to questions such as: Is the data I am storing identifiable? What deletion capabilities exist within my systems? How can data protection compliance be proven to a regulator?

This is easier said than done. Most companies admit difficulties with fundamental questions of records management. Major challenges arise when setting up data governance, defining clear goals and responsibilities and practising these within the company, choosing the right controls, and monitoring new data or changes in data processing. Furthermore, many companies in Europe admit that they do not have a clear data architecture or data quality principles in place.

At PwC, we have developed a field-tested approach for conducting a data minimisation project from end-to-end. We present this approach below, alongside an overview of the main challenges normally faced by Swiss companies. This paper is focused on data minimisation but addresses the topic from a data and records management perspective.

1 Source: Forbes, May 2018

2 Regulatory background

Spearheaded by the European Union, the importance of data protection is increasing dramatically for regulators and companies worldwide

2.1 Data protection in the EU – GDPR

With the accelerating pace of digital transformation and the ubiquitous proliferation of data processing technology in every realm of society and economy, data and records management are taking centre stage and becoming a top priority for both regulators and companies. Organisations process ever-increasing amounts of data, and as such they face more and more rigorous regulatory and operational requirements to safeguard the security and privacy of their data and to protect their operations and their customers' rights.

Spearheading a global wave of new regulations aimed at protecting the personal data of individuals, the European General Data Protection Regulation (EU GDPR) came into effect on 25 May 2018. As GDPR has introduced a paradigm shift when it comes to the processing of personal data and transparency, many companies are still struggling with GDPR compliance more than one year after its date of application.

In line with the new regulation, the Data Protection Authorities (DPAs) can impose financial penalties for infringements of up to 4% of the global annual revenue of the prior financial year, or EUR 20 million, whichever is higher. We have seen record penalties as a result, such as the most recent fines imposed by the UK International Commissioner's Office (ICO) in 2019 on British Airways for more than EUR 204 million and on Marriott International for more than EUR 110 million. Allegedly, British Airways and Marriott were fined for their data security practices that violated the GDPR and ultimately led to data breaches affecting more than 800 million clients overall.

Furthermore, more than 400 cross-border cases are currently being collaboratively investigated among the European authorities. This collaborative approach to investigation might also affect how the appropriate punishment is decided over time.[2]

Figure 1: Fines under GDPR

	Upper Level Infringement	Lower Level Infringement
Total possible fine under GDPR	Up to €20 million, or 4% of global annual revenue of prior financial year (whichever is higher)	Up to €10 million, or 2% of global annual revenue of prior financial year (whichever is higher)
Underlying infringement that can lead to such a fine	• Data processing principles (Art. 5) • Lawful bases for processing (Art. 6) • Conditions for consent (Art. 7) • Processing of special categories (Art. 9) • Data subjects' rights (Art. 12 to 22) • Data transfers to third countries (Art. 44 to 49)	• Conditions for children's consent (Art. 8) • Processing not requiring consent (Art. 11) • General obligations (Art. 25 to 39) • Certification (Art. 42) • Certification bodies (Art. 43)

2 The European Data Protection Board (2019): GDPR in Numbers

2.2 Data protection in Switzerland – FADP

In Switzerland, the EU GDPR is only applicable to companies that process the personal data of data subjects in the EU. The Federal Act on Data Protection (FADP) was introduced back in 1992. Its revision – and thus a stricter regulation of the protection of personal data – is currently under way. The National Council passed the Draft Federal Act on Data Protection (D-FADP) in autumn 2019. At the time of writing, the revision is pending with the Political Institutions Committee of the Council of States. Due to the broad definition of data processing, which includes the collection, storage, safekeeping, use, modification, disclosure, archiving, deletion and destruction of data, only very few companies in Switzerland will be unaffected by the revision.

In view of the severe possible sanctions in the area of data protection (both from GDPR and from FADP), Swiss companies are increasingly investing in data protection compliance, with a strong focus on the “need-to-know” and data minimisation principles – as these are among the most important requirements arising from the regulations. The first step in complying with data protection regulation from a long-term perspective is a comprehensive understanding of the processing and storage of personal data. A thorough understanding of the data processed in your enterprise will reduce the operational effort in the second step on your journey to data compliance: the development of automated deletion capacities in the IT application landscape.

2.3 Regulations for financial services companies in Germany and the Netherlands

For financial services companies located in Germany or the Netherlands, GDPR is the primary regulatory driver when it comes to data and records management, and as an EU regulation is directly applicable without transposition in local law. However, GDPR leaves room for national discretion in certain aspects. To this end, the German Bundesdatenschutzgesetz (BDSG) or the Dutch Algemene Verordening Gegevensbescherming (AVG) further specify the applicable data protection requirements and add their own national flavour. These include the German BDSG's supplementary provisions governing crimes and fines provisions, which stipulate, for example, a custodial sentence of up to three years or a fine for anyone who knowingly discloses the generally inaccessible personal data of a large number of people.

Besides GDPR and its national implementation acts, there are several other (future) regulations with implications for data protection, data governance and data management, such as BCBS239, Basel III and Basel IV, ePrivacy, IFRS17 or even Brexit, which will require financial services firms to ramp-up their data capabilities.

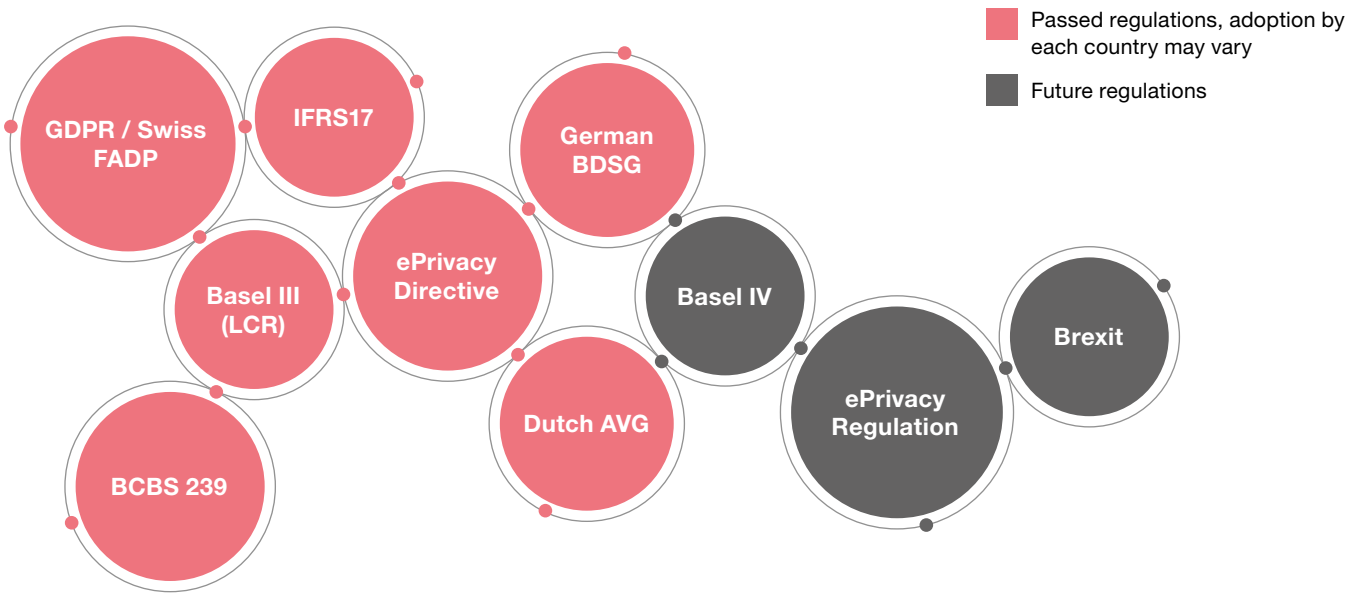
The ePrivacy Rgulation (ePR) will replace the existing ePrivacy Directive[3], which was revised in 2009. The new regulation includes several modifications to address current trends in digital markets and provides for a considerable extension of scope. The key goal of the ePrivacy is to protect electronic communications of natural and legal persons and to protect the information stored in those persons' end terminals. The ePrivacy aims at complementing and specifying the requirements set out in the EU GDPR.

Since the two regulations may have points of overlap, it is important to note that the rulings under ePrivacy are lex specialis to the GDPR and therefore they will prevail over GDPR requirements in case of conflict (provided they do not lower the level of protection enjoyed by natural persons under the GDPR). In November 2019 the latest draft was rejected once more, resulting in a further delay of the ePrivacy adoption. The impact on Switzerland depends heavily on the detailed implementation of the EU Member States.[4]

With BCBS239, the Basel Committee on Banking Supervision requires G-SIBs[5] to adhere to their principles for effective risk data aggregation and risk reporting. It includes four areas: governance and controls, risk standards and processes, infrastructure and architecture as well as data management. While initially aimed at institutions designated as G-SIBs, BCBS 239 has become a de facto standard across the banking industry and several national supervisors are now formally requiring D-SIBs[6] under their jurisdiction to be compliant.

Acknowledging the multitude of relevant regulations on international, European and national level, financial services firms are advised to consider a Gap Assessment to better understand their current data and records management operations and identify potential gaps so they can comply with the applicable regulatory requirements. This helps to focus on the most pressing elements and to maximise the impact of your efforts.

Figure 2: Overview of general European and local legislation



3 Directive 2002/58/EC and the 2009 update, Directive 2009/136

4 Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB); E-Privacy (Transparenz im Internet).

5 Global systemically important banks (G-SIBs)

6 Domestic systemically important banks (D-SIBs)

3 Implementing state-of-the-art data minimisation capabilities as part of data and records management

Moving beyond the regulatory requirements, the implementation of state-of-the art data and records management represents an opportunity to transform a company's core operations and culture into a digitally intelligent organisation that allows it to make better decisions and to stay ahead of the curve.

Embarking on a data minimisation journey as an integral component of data and records management can seem daunting at first, considering the staggering amounts of data, complex IT landscapes and increasing regulatory requirements. The benefit of a data minimisation initiative is data protection compliance. The journey to data minimisation starts with the major task of understanding the system landscape and the IT-infrastructure.

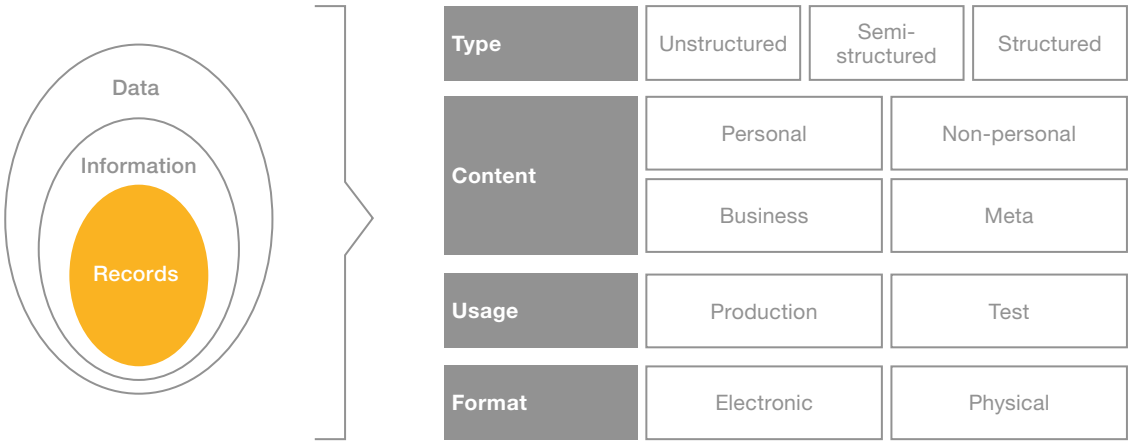
Set the scope of your data management initiative early in order to precisely plan resources and costs

3.1 Defining the scope of your data and records management initiative

It is important to define the scope of your data management initiative right at the outset so you can focus your efforts on the areas that matter the most to you. To help you on this journey, we have developed the "PwC Data Egg", which is a simple yet effective instrument to identify the core needs of your stakeholders. It also allows you to develop a shared vision to facilitate a successful transformation.

As the foundational layer of the PwC Data Egg, **"Data"** can be defined as raw, unprocessed statements, e.g. a representation of an objective fact. In today's digital world, data is the lifeblood of our economy, but it is important to understand that data itself has no significance beyond itself. It is through processing, mining and contextualising that data can be comprehended and turned into **"Information",** which enables better decision-making.

Figure 3: The PwC Data Egg

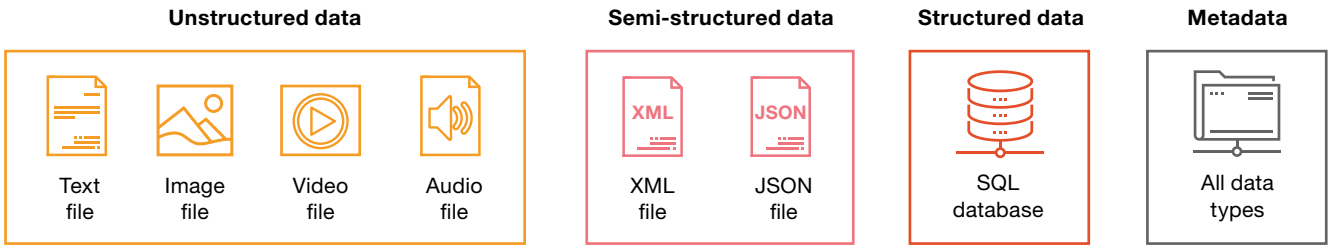


In pursuit of a firm's legal or business obligations, it is often necessary to preserve an account of past events; to provide objective evidence of business activities, transactions performed, events occurred, statements made, or results achieved. For this purpose, "Records" – consisting of one or more documents collectively forming an unalterable state of a document – are indispensable. Since records often represent vital business information, it is essential to safeguard them with adequate technical and organisational measures, while providing access to them on a limited, need-to-know basis.

Attributes for selecting the scope of the data layer subject to your data management initiative

When defining the scope of your data and records management initiative, you should focus on the key attributes of the data layer, as summarised below. While the PwC Data Egg represents a good starting point to define the scope of a data and records management initiative, experience shows that an in-depth analysis is often necessary to get a clear understanding of a company's current data landscape and to set the right priorities.

Figure 4: Example of data types



Data type

At the data layer, three different data types can be differentiated: unstructured data, semi-structured data and structured data. Structured data is organised in a predefined data model, usually in tabular format with a relationship between rows and columns such as an Excel or SQL database.

Semi-structured data can be considered a special type of structured data, which is not organised in the formal structure of relational data models but features some sort of hierarchical structure, enforced through semantic elements such as semi-columns. This allows semi-structured data to be transformed into structured data. Hence, the analysis of semi-structured data requires considerably less effort than unstructured data.

By contrast, unstructured data does not adhere to any predefined data model or hierarchical structure, making it difficult to analyse using conventional methodologies. Common examples of unstructured data include text files, such as for example Word or PowerPoint files stored on a shared drive; but also images, videos or audio files. In recent years, new technologies and tools in combination with continuously growing (cloud) computing power have facilitated the analysis of unstructured data.

Ultimately, the scope of a comprehensive data and records management initiative should encompass all the three data types mentioned above. This might not be possible for most organisations at first due to resource constraints. Therefore, we recommend starting with structured data to satisfy regulatory requirements and demonstrate the value to your key stakeholders. Subsequently, the scope can be gradually expanded according to a risk-based approach form semi-structured data to different types of unstructured data.

Data content

From a regulatory-driven data protection perspective, personal data was and still is at the heart of most data and records management initiatives, since violations of personal data protection laws can result in considerable financial or reputational fallout. However, from an operational resilience perspective[7], other data domains are equally important for your company's core business. As most industries today are extremely data intensive, it is vital to ensure high data quality, continuous data availability and consistent data management.

It is also important to distinguish between the business data itself and so-called metadata, which refers to data about the data and provides additional information about the properties of a specific data structure or record such as its author, date of creation or technical field requirements.

While we do not recommend restricting the scope of your data and records management program in terms of data content, potential scope limitations could exclude ancillary data domains that are not vital to your core business. In every case, close alignment with the respective business representatives is indispensable.

Data usage

Other considerations include the question of whether to include test data in the scope of a data and records management initiative. While production data clearly has a higher operational relevance, we recommend that test data should not be systematically excluded, as this can lead to complex clean-up activities in the future.

Data format

Ultimately, a decision has to be made concerning the extent to which physical data (documents in physical form) is included in the scope of such an initiative, as this usually also requires more manpower and a somewhat different skills set. As electronic data is often also stored physically, we recommend including physical data into the analysis to identify dependencies and storage locations of the data in scope. However, the clean-up of physical archives and other storage locations is best addressed with independent project organisations, as it runs on a different timeline and involves different resources.

7 For more information on the topic of operational resilience, please refer to **PwC (2019) Operational resilience – your Swiss army knife to survive the next crisis.**

3.2 Risk-based approach to implementing data minimisation capabilities

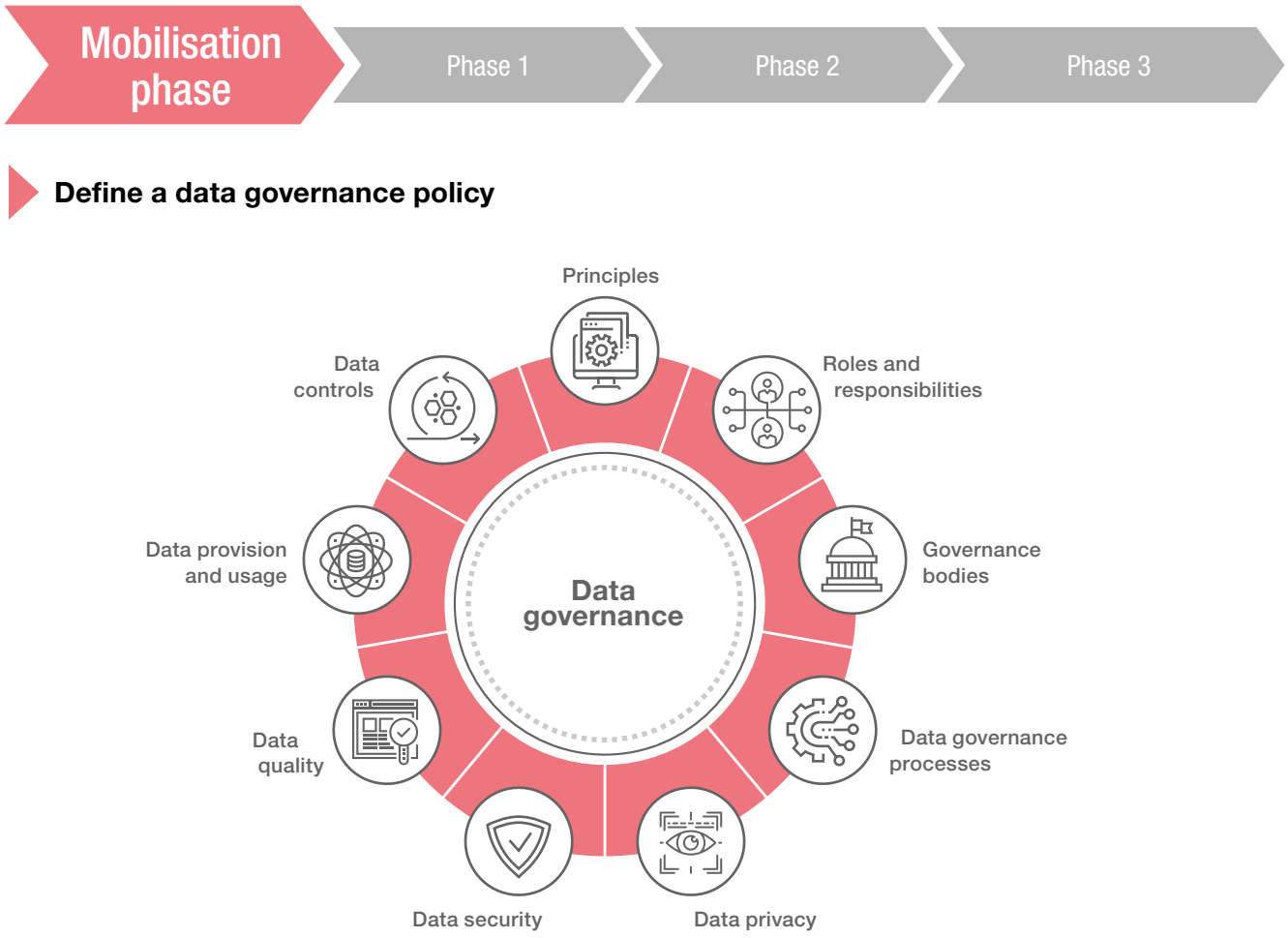
Many medium-sized and large companies maintain a large application landscape with hundreds or even thousands of applications. At times, companies show a lack of basic knowledge about the applications, which data they process and the direction of the data flow, as well as the interfaces connecting them. Having established a comprehensive data governance framework, an analysis of the application landscape lays the foundation for planning and implementing deletion capabilities. Figure 5 illustrates PwC's proven approach for a data and records management initiative to implement data minimisation capabilities, which will be further detailed in the following sections.

Figure 5: High-level approach for the implementation of data minimisation capabilities

3.2.1 Mobilisation phase – Data governance framework

Before starting a data minimisation project, it is essential to establish the necessary prerequisites by implementing a comprehensive data governance framework (if not defined already).

Figure 6: Mobilisation phase – Data governance framework



Defining roles and responsibilities prior to the data minimisation project will pay off in reduced complexity

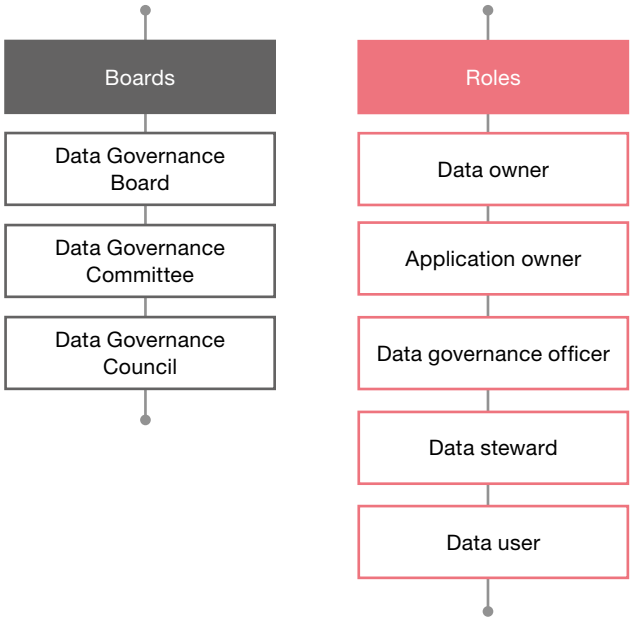
A data governance framework defines clear roles and responsibilities to ensure accountability for data collection, processing and storage, as well as adequate data quality standards. Aligned to a company's data strategy, such a framework defines the scope and guiding principles of data governance activities in an organisation and enables consistent and efficient data management across geographies and business units.

A key element of a data governance framework is the formalisation and implementation of a data governance organisation, consisting of data governance bodies and data governance roles. Each of these governance bodies and roles is associated with a designated set of responsibilities, and collectively they facilitate the operationalisation of the data governance framework.

It is important to note that the specific roles and responsibilities and the corresponding operating model are heavily dependent on an organisation's business needs, digital maturity and culture. For each role, there must be an extensive role description, responsibilities and processes, controls and competences. There is a standardised industry approach to doing so, which is why this will not be discussed further within the scope of this paper.

Below is an overview of archetypical data governance bodies and roles:

Figure 7: Overview archetypical data governance bodies and role



In the absence of clearly defined ownership and accountability, the complexity of any data-related initiative increases exponentially – and with it, the risk of failure. Without a clear owner structure, responsibilities are not clear and the completion of tasks from a data, system and application perspective becomes lengthier.

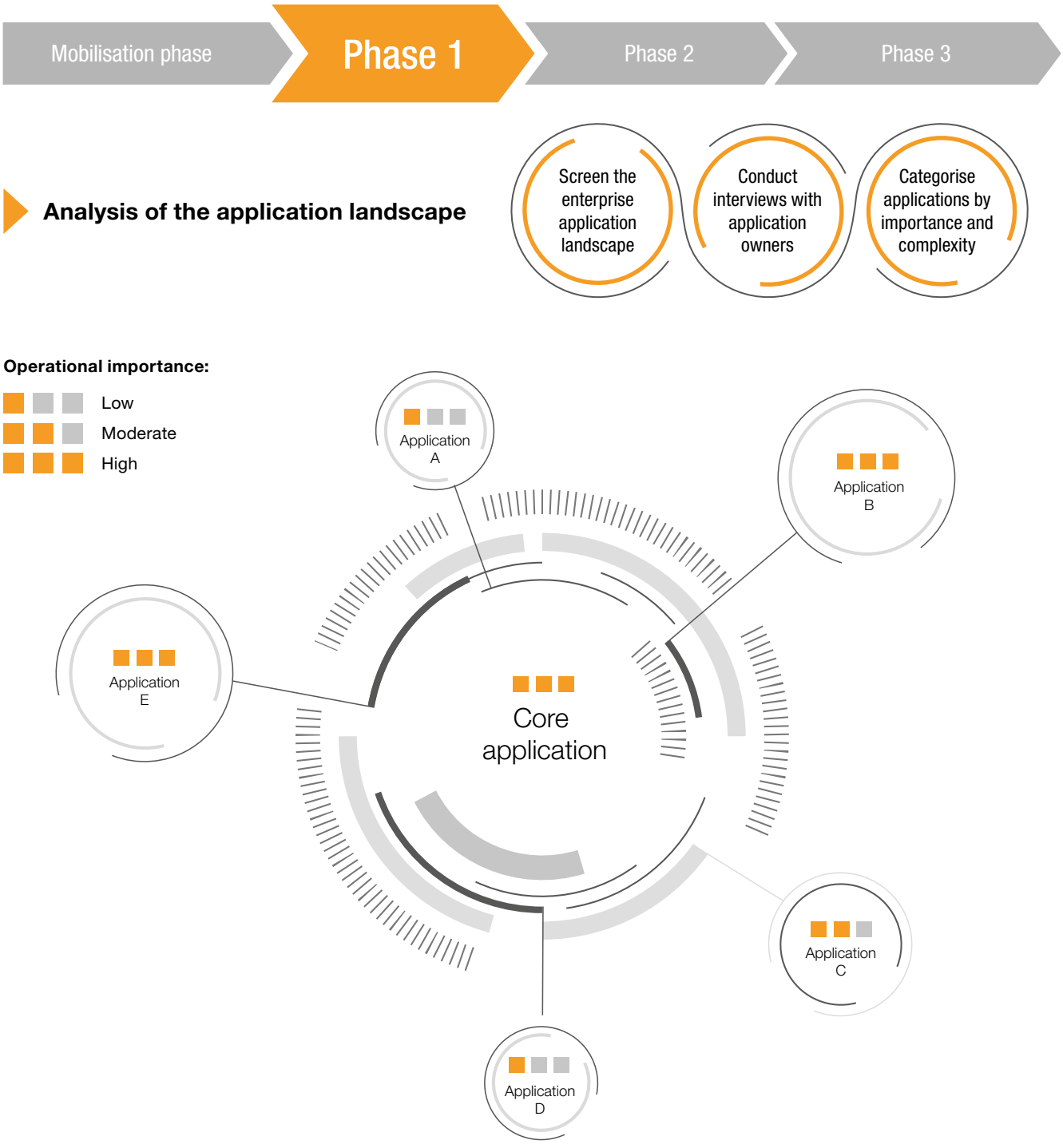
3.2.2 Phase 1: Analysis of the application landscape

In phase 1, a risk-based assessment of data processing in your application landscape is performed, usually including three main activities:

1. Screen the enterprise application landscape
2. Conduct interviews with application owners
3. Categorise applications by operational importance and complexity

Building an inventory of your application landscape and the associated data setup

Figure 8: Analysis of application landscape



The assessment results in an overview of the application landscape and its associated data processing, providing you with a comprehensive picture of your applications, prioritised by operational importance and complexity (risk-based approach). This approach ensures prioritisation of your resources across the organisation's applications, so you can start by addressing the highest risks in relation to data minimisation.

Figure 8 provides an illustrative example of the prioritisation of several applications connected to the company's core system.

Screening of the enterprise application landscape

As a first step, it is crucial to understand the organisation's application landscape, including every single application. Thus, it is important to understand each application's functionality, the interfaces connecting them and which of the applications are relevant in terms of data protection. You should also understand if an application will remain operative or whether there is a plan to decommission the application in the medium term. At this stage, it is crucial to identify the applications which process personal data. Among them you want to determine the data sources, how relevant data is processed, how long it is stored and where it is distributed to.

At this stage of the analysis, each application should be scored by "importance". Two factors must be considered for determining the overall importance of any application:

1. Operational importance – This can be evaluated by answering a simple question: Could the company pursue its core business without the application?

2. Data protection criticality – Different factors should be taken into consideration here, for example if sensitive data is being processed and whether personal data is stored in physical format. It is important to involve a personal data protection expert at this stage to make sure you ask the right questions so you can adequately assess the importance of the application.

Conduct interviews with the application owner to support your findings

After the initial assessment, it is essential to interview the application owners to clear up any misunderstandings and make discoveries beyond the standard questions investigated in the previous steps.

Categorise applications by importance and complexity

After the interviews, you will have gathered enough information to perform a cluster analysis of your applications. It is unlikely that an organisation has enough time and budget to address all applications at once. Hence, a risk-based approach is suggested to prioritise the applications. The most important factors taken into consideration for clustering are the complexity of implementing a deletion function as well as the (data protection-related) importance of the application, as described above.

The As-Is maturity of an application's deletion capabilities determines the complexity going forward. The most mature applications have capabilities to delete data protection-relevant data automatically after a predefined period. Less mature applications have only a manual deletion capability. For such applications, the implementation of automated deletion capabilities can potentially be postponed. However, manual deletion is not only costly but also error-prone. The least mature applications have no deletion capabilities at all and should be prioritised in a data minimisation initiative if such applications process personal data.

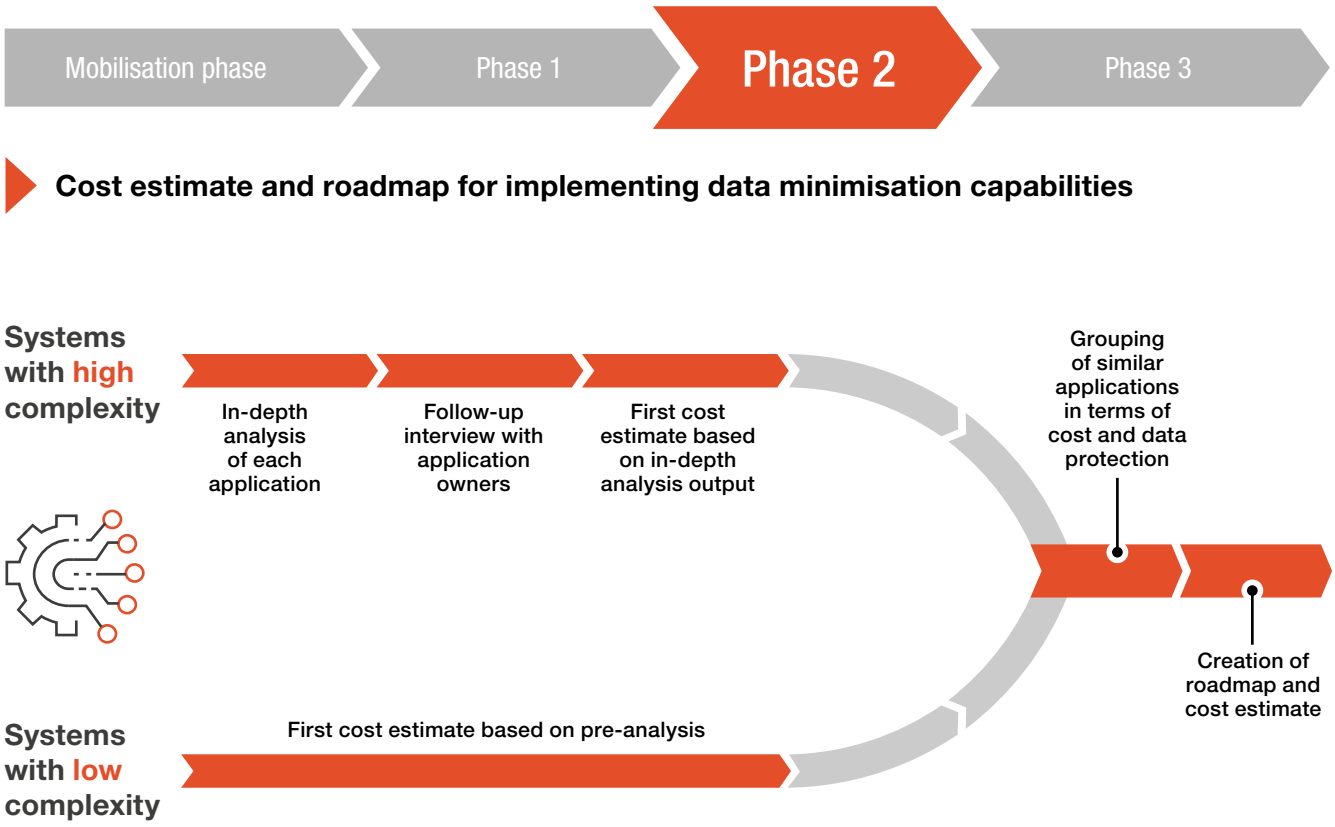
The combination of complexity and overall importance determines an application's criticality and hence the final suggested prioritisation.

3.2.3 Phase 2: Planning and roadmap for data minimisation

Phase 2 focuses on planning the implementation of data minimisation and deletion capabilities across all the applications included in the scoped of the previous phase. The key output here is to define the To-Be state for each application, and the cost/time/resource estimate for reaching such target.

The level of complexity of each application is a key component to define your delivery roadmap

Figure 9: Planning of roadmap for data minimisation



At this point you may encounter highly complex applications and other challenges such as dependencies on other systems within the organisation. Dependencies to external software providers make the environment even more complex and can be highly time-consuming. It is therefore advised to take this into account when developing your roadmap and to identify at an early stage which applications are potential bottlenecks. You can then analyse the dependencies of those applications and incorporate the resulting impact into the roadmap.

When it comes to estimating the costs of implementation, it is beneficial to break down the individual costs involved. Thus, we recommend splitting the costs into continuous (run) costs and one-time costs. Continuous costs are usually relatively small in comparison to one-time costs needed to develop deletion capability. However, accumulated run costs can make a difference.

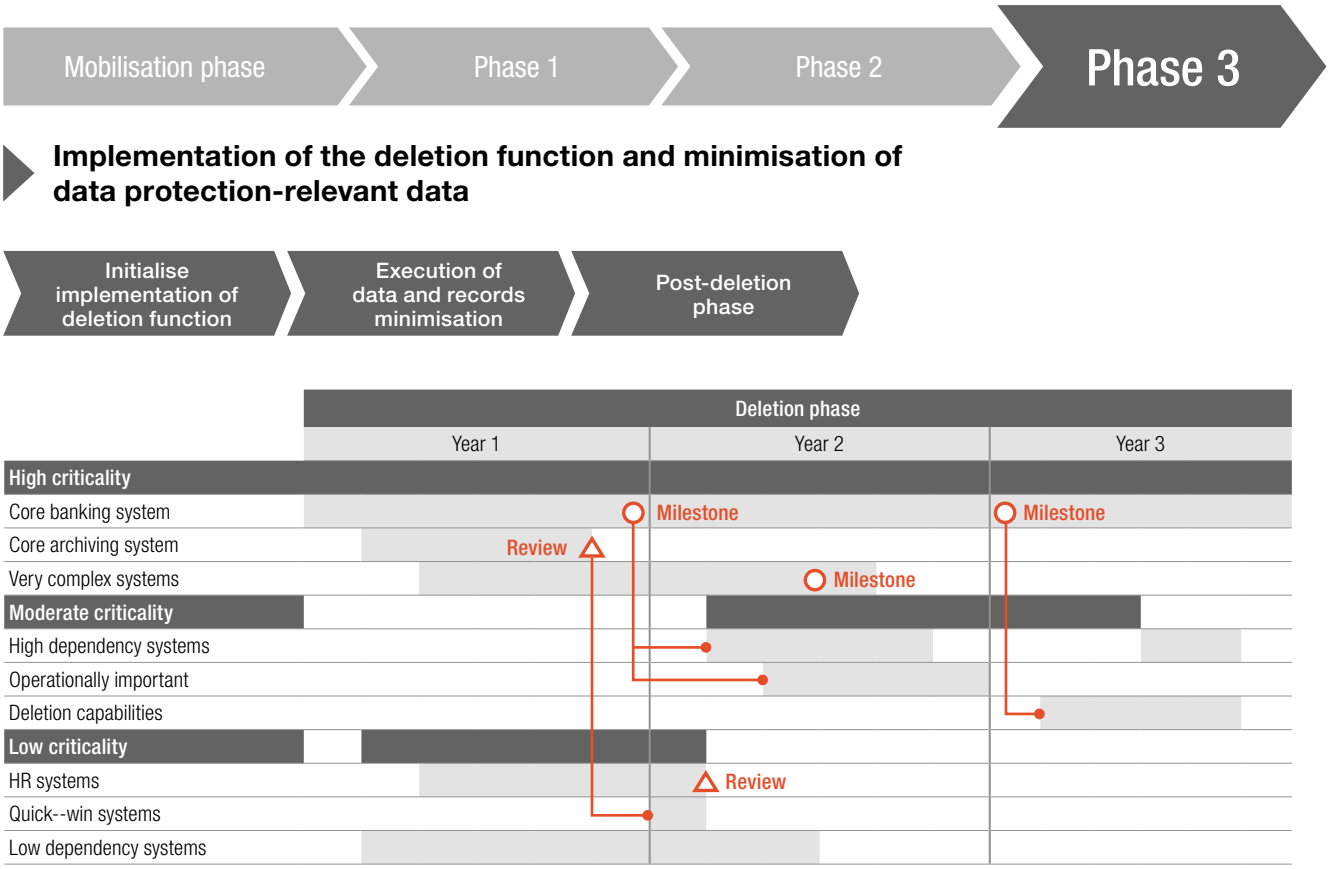
Therefore, it is important to estimate how many times you will have to run your deletion process. When it comes to defining the To-Be state, it should be remembered that data security and data protection can be ensured by balancing requirements and possibilities within the legal framework. If, for example, deletion is not an option for the organisation (e.g. due to cost or operational constraints), the possibility of anonymisation can be evaluated instead in order to ensure compliance with data protection rules.

3.2.4 Phase 3: Implementation of data minimisation and deletion capabilities following a risk-based approach

Phase 3 focuses on the implementation of the data minimisation and deletion capability. Implementation should follow the roadmap created in the previous phase, and as such it should focus on the most important and critical applications first and consider interdependencies across the applications.

Focusing first on highly critical applications as well as "proof-of-concept" applications will simplify your life going forward when executing data minimisation

Figure 10: Implementation of data minimisation and deletion capabilities



Applications with a low overall importance generally show a significantly lower level of dependency and complexity. They are often referred to as quick wins as the deletion function can be implemented rapidly. For these reasons, they are convenient candidates for pilots or a proof of concept. Pilots on simple applications are very useful in order to test the deletion capability of applications and the behaviour of connected processes. Because pilots and proof of concepts are subject to change, it makes sense to address those operations at the beginning of data minimisation, as shown in Figure 10. Changes to the minimisation process can be detected at an early stage, and mistakes do not affect the broad mass of moderately critical applications. It is just as important to deal with high-criticality applications from the beginning. The high interdependency with other systems, third-party providers or complex technical environments of the applications itself can easily cause bottlenecks. The earlier issues with these applications are detected, the better.

An important part of this phase is the communication of minimisation plans. Relevant stakeholders must be informed about major changes to the applications they are using, and which processes will be affected by the data minimisation. Ideally, key stakeholders should be involved in the decision-making process. This often ensures smooth implementation and keeps resistance to the change to a minimum.

In this phase, the roadmap developed in phase 2 is put to the test. The actual execution of data minimisation depends on the planning phase and on the complexity of the system. Are external providers or implementation partners involved in the process? If so, the complexity of minimisation rises. In some cases, legacy systems or legal restrictions can affect the minimisation effort, which is why preparation makes a huge difference to the success of this phase.

The last phase is completed once the deletion process is implemented and contains all activities after the actual deletion. This includes functional support and guidance ensuring sustainable data compliance of the new setup. It is recommended to define KPIs (i.e. the volume of deleted data per retention cycle) and to run tests across the entire IT landscape. Control measures like this will allow you to determine the rate of success of the deletion process and to plan the next retention cycle accordingly.

Automated deletion capabilities

The automated deletion process should be triggered by a periodical event and should identify and preselect the relevant personal data in the database of the application. Specific data should be excluded from the deletion process due to a predefined exception rule (e.g. legal hold when data is needed for an ongoing legal case). After all relevant data has been selected (both in the application and in other connected applications such as backup systems), the deletion process will be executed. It is also advisable to introduce a process to archive the report, since it may be required later on to support comprehension and provide proof of successful deletion. In a perfect world, the deletion process is entirely automated based on a predefined rule set. However, the realisation of this deletion function is not feasible/cost-effective for every application.

4 Typical challenges observed in the journey to better data and records management

Four key challenges that might be a threat to your data protection initiatives if not tackled beforehand

Thanks to our experience in the field, we can help you identify potential challenges early on in the process to ensure you are prepared to tackle them and you can successfully deliver the changes needed. Below we illustrate some of the typical challenges you may face.

4.1 Insufficient ownership of the IT landscape

Challenge

Lack of the required know-how as well as decision-making power leads to inefficient and ineffective implementation of a successful data management initiative. In the worst case, this ends in a non-sustainable handover to business as usual.

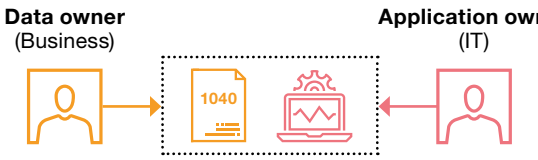
Root cause

Insufficient ownership and accountability of the IT landscape, i.e. no clearly defined governance roles and associated responsibilities.

Best practices

1. An organisation needs to define and implement governance roles with their corresponding responsibilities that are fit for purpose and suit the existing governance model.
2. From a data and records management point of view, there is usually a data perspective and an application perspective that needs to be considered. In times of increasingly blurred boundaries between business and IT, it stands to reason that only close collaboration between these two functions can lay the foundation for successful value creation over the long term – as described in the next picture.
3. It is crucial to maintain an up-to-date list with all data and application owners, which is stored centrally and easily accessible by all employees. In order to mitigate natural staff fluctuation within an enterprise, a standardised process needs to be established to identify and appoint suitable data and application owners.

Figure 11: Ownership in the IT landscape



Key responsibilities

- Accountability for data quality, data controls and data lineage for the data they own
- Provides a mechanism for discussing, agreeing and delivering on data requirements from data consumers
- Ensures processes and procedures are in place to prioritise, address and resolve data quality and other related issues
- Reviews the existing data control framework of their unit for the data they own and raise issues

Key responsibilities

- Manages the application change management process throughout their lifecycle
- Facilitates the process by providing information about the application's business use, placement in the broader business process to the right people and information, including discussions with third parties if the application is vendor-developed or hosted
- Maintains application information, checks eligibility and operates the application

4.2 Dependencies on third-party providers

Challenge

Depending on the application type and the chosen implementation model, a number of different internal and external dependencies can occur, increasing complexity and thereby potentially having an adverse impact on the timing, cost or quality of the transformation.

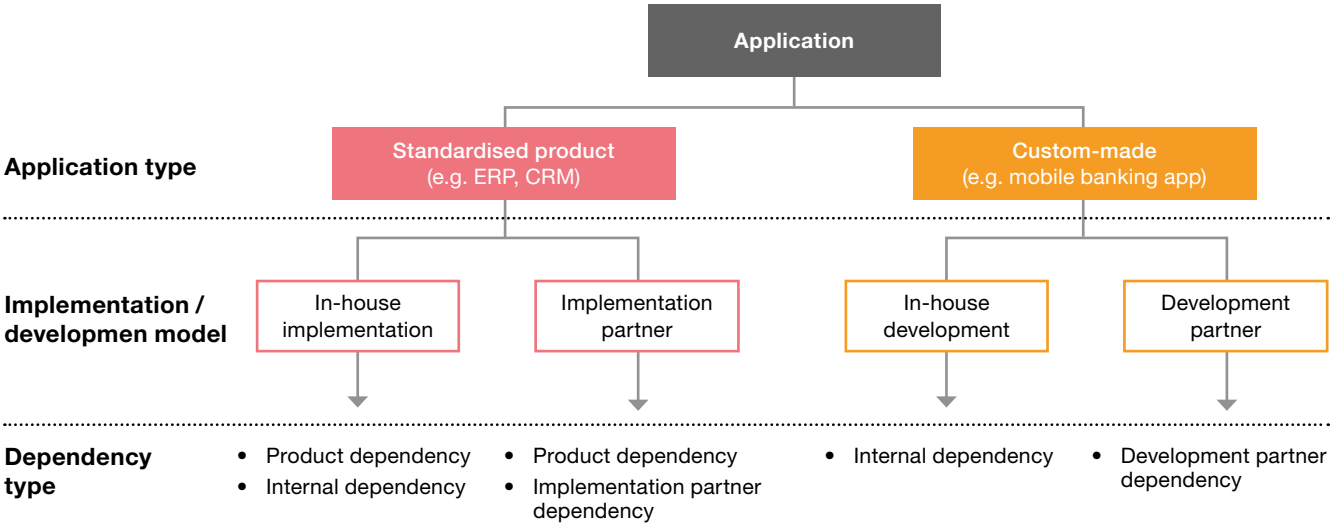
Root cause

Outsourcing of application development or implementation to third-parties.

Best practices

1. Analysis of application inventory to identify:
   - Standardised software products such as ERP or CRM systems provided by a product vendor or implemented by an implementation partner
   - Custom-made applications developed by a development partner
2. Clarification with product vendor to determine if, when and how the desired functionality can be provided. In the best case, the vendor has already developed a corresponding module to ensure compliance of their software with certain regulatory requirements, while keeping your development and integration effort to a minimum. If this is not the case, the vendor might be interested in co-developing such a module. In the worst case, it is technically not feasible to implement the required feature, forcing a software change.
3. Clarification with internal implementation teams and external implementation partner to establish whether required resources are available. Theses clarifications should be executed in a decentralised fashion by application owners and other subject matter experts, while providing comprehensive on-demand legal and methodological support through the data protection office and the project management function.

Figure 12: Understanding internal and external dependencies



4.3 Processing of unstructured and physical data

Challenge

When processing unstructured and physical data, it is hardly possible to enforce compliance with data protection principles such as data access rights or automated deletion capabilities. This exposes companies to significant data protection and security risks.

Root cause

Limited technical measures allowing companies to manage and control the processing of unstructured or physical data.

Best practices

1. Implementing a comprehensive data governance framework providing clear guidelines on how to process unstructured and physical data along the entire data management lifecycle and the responsibilities associated with this forms the cornerstone of every data and records management initiative and creates the required legitimacy for further actions.
2. Adopting a strategic view, the processing of unstructured and physical data should be gradually reduced as part of a company's digital transformation program. In order to optimise a company's resource allocation, it is recommended to follow a risk-based approach.

Complementary, tactical measures such as scanning tools or data cataloguing can help reduce the risk exposure more rapidly.

4.4 Decommissioned applications

Challenge

Decommissioned applications are no longer in operative use, but oftentimes they still store (potentially sensitive) personal information, mostly due to legal hold requirements. As the implementation of technical data protection measures such as automated deletion capabilities is often not economically viable for decommissioned applications, manual deletion and data cleaning procedures have to be defined and executed on a periodic basis.

Root cause

Legal hold requirements prevent deletion of data in decommissioned applications.

Best practices

1. Include decommissioned applications in the scope of the initial analysis of a data management initiative. As decommissioned applications are old applications, most of which will have been substituted by new applications, often they hold legacy data, e.g. data that is older than ten years. This particularly increases the data protection compliance risk for an organisation.
2. Analyse whether it is economically viable and technically feasible to migrate the remaining (personal) data from the decommissioned application to another application.
3. If no migration of the remaining personal data in the decommissioned application is planned, a periodic review of the relevant legal hold requirements has to be conducted in collaboration between the architecture team, the legal department and the data protection office. In this process, the following key questions need to be addressed and documented in an auditable fashion:
   - What type of data is stored and why?
   - What is the retention period?
   - Who is the owner of the data?
   - What is the deadline for deletion and who is in charge?
4. Set up an approval process that allows for a periodic check of all decommissioned applications in the organisation. The idea of such an approval cycle is to answer the questions above and to challenge requests for extension of retention of non-relevant personal data. Another objective is to ensure that all accountable departments (legal, data protection, etc.) know about the existence of decommissioned applications as well as the reason for their data retention.

5 Call for action

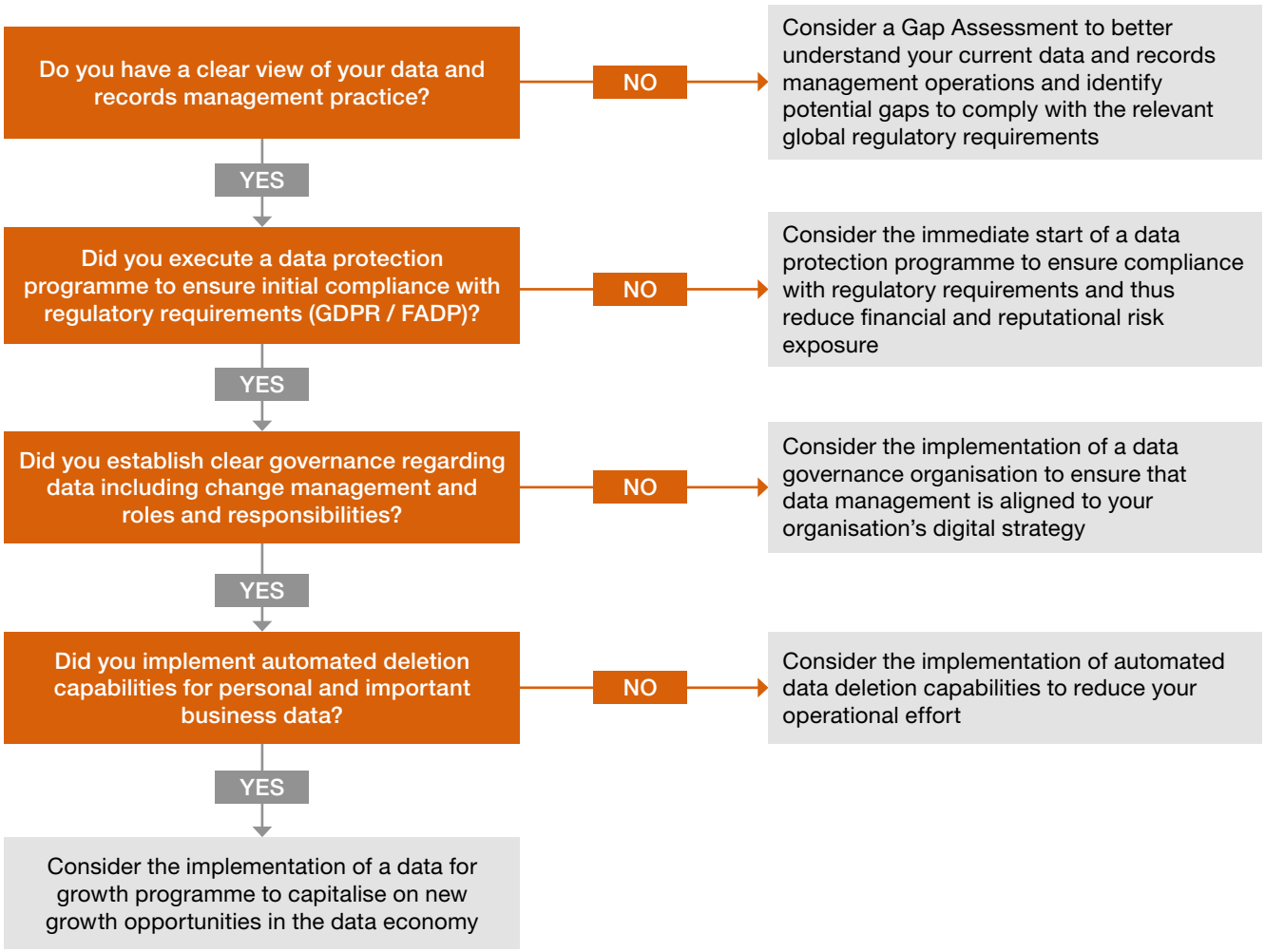
Depending on the level of data protection compliance your company has reached, there are several action points

5.1 Decision tree: Where do you stand on your data and records management journey?

Data and records management has been on companies' agendas for many years now, mainly with a focus on increasing operational efficiency. In addition to this, and as a result of the recent global regulatory push for improved data protection, businesses are now being formally required to revise their current data and records management practices in order to establish the basis for a successful future in the digital age and ensure compliance with the updated regulations.

Navigating the multitude of different yet interrelated initiatives centred around data and records management and data protection can be challenging. Our decision tree can provide a useful starting point to assess where you stand on your data and records management journey.

Figure 13: Decision tree to assess your position on your data and records management journey



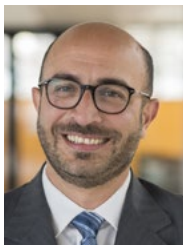
The steps in the decision tree should not be viewed in isolation. Rather, they should be considered as stepping-stones on your journey to data protection compliance, where earlier steps must be in place before continuing with the next step. The target is to have implemented automated deletion capabilities for your data. Once you have met the regulatory requirements and implemented automated deletion capabilities, the next step to capitalise on your enterprise data is a data for growth program.

A data for growth program helps you identify new trends and developments, use creative methods and deploy innovative technologies to derive the maximum benefit for you – not just today, but in the future as well. With radical innovation and design thinking, we ensure that you recognise major trends, revolutionise procedures and pinpoint the goals that matter to you.

5.2 How can PwC help you?

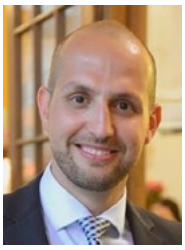
Data protection regulations and data and records management are two realities that no business can afford to ignore. PwC offers your company a tried-and-tested approach and leverages transformation capabilities to support you on your journey to data protection compliance. We can also help you develop the agility and the mindset necessary to respond to rapidly changing regulations in this context. You will gain unique, value-added solutions backed by industry and technical expertise and our collective experience from across PwC.

For more information please contact our experts



Patrick Akiki
Advisory Partner, Finance Risk
and Regulatory Transformation

+41 79 708 11 07
akiki.patrick@ch.pwc.com



Morris Naqib
Director, Finance Risk
and Regulatory Transformation

+41 79 902 31 45
morris.naqib@ch.pwc.com

Stephen Strebel
Director, Advisory

+41 79 821 12 92
stephen.strebel@ch.pwc.com

Philipp Schwarz
Assistant Manager, Advisory

+41 79 120 54 81
philipp.schwarz@ch.pwc.com

Emanuel Staubli
Consultant, Advisory

+41 79 709 10 49
emanuel.staubli@ch.pwc.com

Key contributors

We would like to thank Isabella Sorace for her valuable contribution to this publication.

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00