www.pwc.ch

The ever-evolving challenges for records and data management

Records and data management in times of new data protection and privacy standards, legal hold and retention schedules

pwc

April 2019

Companies that have not yet revisited their records and data management should put this at the top of their agenda.

A journey for all kind of structured and unstructured data

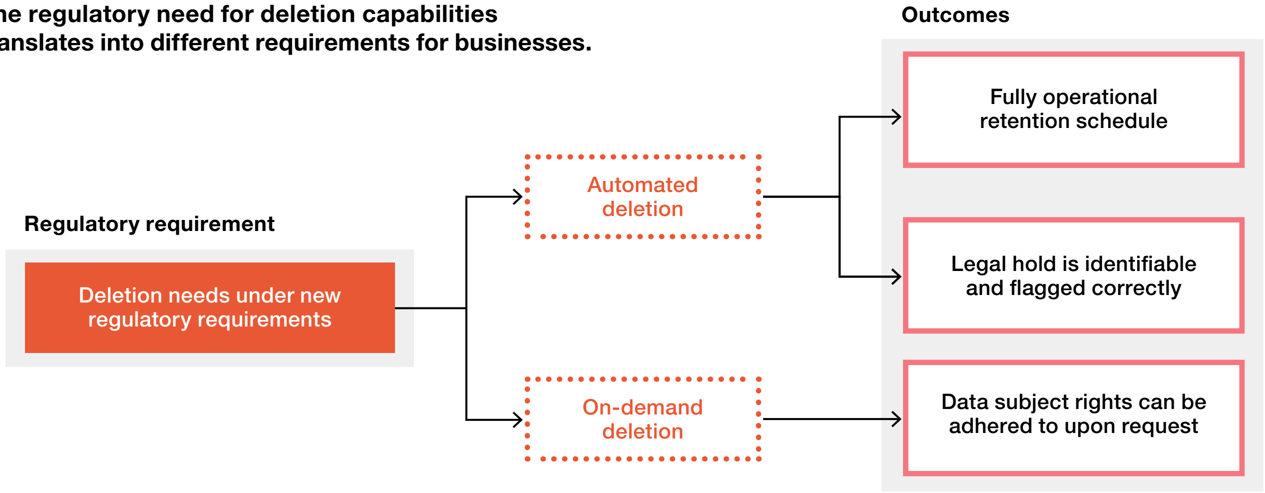
Records management and adherence to legal hold and retention rules when managing data has always been a key element of a company's daily business.

The expected revision of the Swiss Federal Act on Data Protection (FADP), combined with EU ePrivacy and the EU GDPR, means data management is subject to even more requirements. In the wake of the EU GDPR, deletion and data identification have become a central focus.

Being able to understand what data a company processes, how it is maintained and be able to identify and delete it is key to efficiency and future compliance.

In the post-GDPR world, it is important not to limit the improvement of records and data management to personal data only. This should be a journey for all kind of structured and unstructured data.

The regulatory need for deletion capabilities translates into different requirements for businesses.


Outcomes
Regulatory requirement
Deletion needs under new regulatory requirements
Automated deletion
On-demand deletion
Fully operational retention schedule
Legal hold is identifiable and flagged correctly
Data subject rights can be adhered to upon request

It is important to ask yourself where you stand in terms of records management. The following questions (not exhaustive list) will help you find out:

- What personal data do we process and in which applications and systems?
- Do we know where data is stored within our organisation?
- Do we know what data we archive? Do we ensure that archived data is no longer stored in applications?
- Do we have automated deletion capabilities to ensure adherence to retention periods? Have we considered legal hold rules?
- Do we have a deletion capability for applications, archives and storage units that ensures our adherence to data subject rights and data protection officer requests?

The answers to these questions can help you pinpoint the action you need to take to comply with the new regulatory standards. Experience from the EU GDPR – almost a year after its go-live in May 2018 – has shown that the compliance and efficiency journey for records and data management is long and challenging.

Inadequate record management can become expensive

Regulations like GDPR clearly ask organisations to ensure adequate management of their records, specifically in relation to personal data. But GDPR is not the only regulation in this regard: ensuring your records (both structured and unstructured) are managed in line with the latest technological standards will help you avoid expensive fines from regulators. This is highlighted by the recent example of Facebook, which is facing a record fine for alleged privacy violation after the Cambridge Analytica case of improper record management.

What needs to be considered to ensure compliance with key regulatory requirements throughout the records and data management life cycle

Structured data

Unstructured data

Records management life cycle	Ensure transparency	Ensure privacy by design and default	Respond to requests (internal and external)	Ensure accountability and ownership
1 Data collection	- Timely notification of data collected	- Only data that is necessary for the purpose is collected - Collection of consent (where needed)		- Data is collected following a pre-defined process with clear accountability
2 Data storage	- Identification of data stored (structured and unstructured) - Build and maintain data inventory	- Storage limitation rules set-up - Data accuracy - Data encryption and pseudonymisation	- Retrieve structured and unstructured data stored upon request (data subject requests, legal requirements etc.)	- Data ownership clearly defined - Access management to data clearly defined
3 Data processing and identification	- Identify and maintain what data is processed by which application/system (CID, sensitive data, personal data etc.)	- Data processed only for specified purpose(s) - Data accuracy - Data encryption and pseudonymisation	- When data subject request is received, ensure all processing activities linked to the data are taken into account (including “Pack-up” processes)	- Data processing defined (process owner) - System/ application owner defined - Access management to data defined
4 Data transfer	- Identify and maintain overview of what data is transferred to third parties, internally, outside EU etc.	- Data minimisation - Purpose limitation - Data accuracy - Data encryption and pseudonymisation	- Enable instruction to third parties to adhere to requests (based on the transfer overview maintained)	- In transfer agreement, include clear accountability clauses - In transfer agreement, define access limitations to transferred data
5 Data archiving, retention and automated deletion	- Document types clearly linked to data types – which documents contain personal data/ sensitive data/confidential data	- Data minimisation - Purpose limitation - Link legal hold to archived documents with data disposal (automated deletion) - Data encryption and pseudonymisation	- Retrieve archived data upon request (data subject requests, legal hold etc.) - Ensure deletion of archived data upon request	- Access management for archived data strictly defined

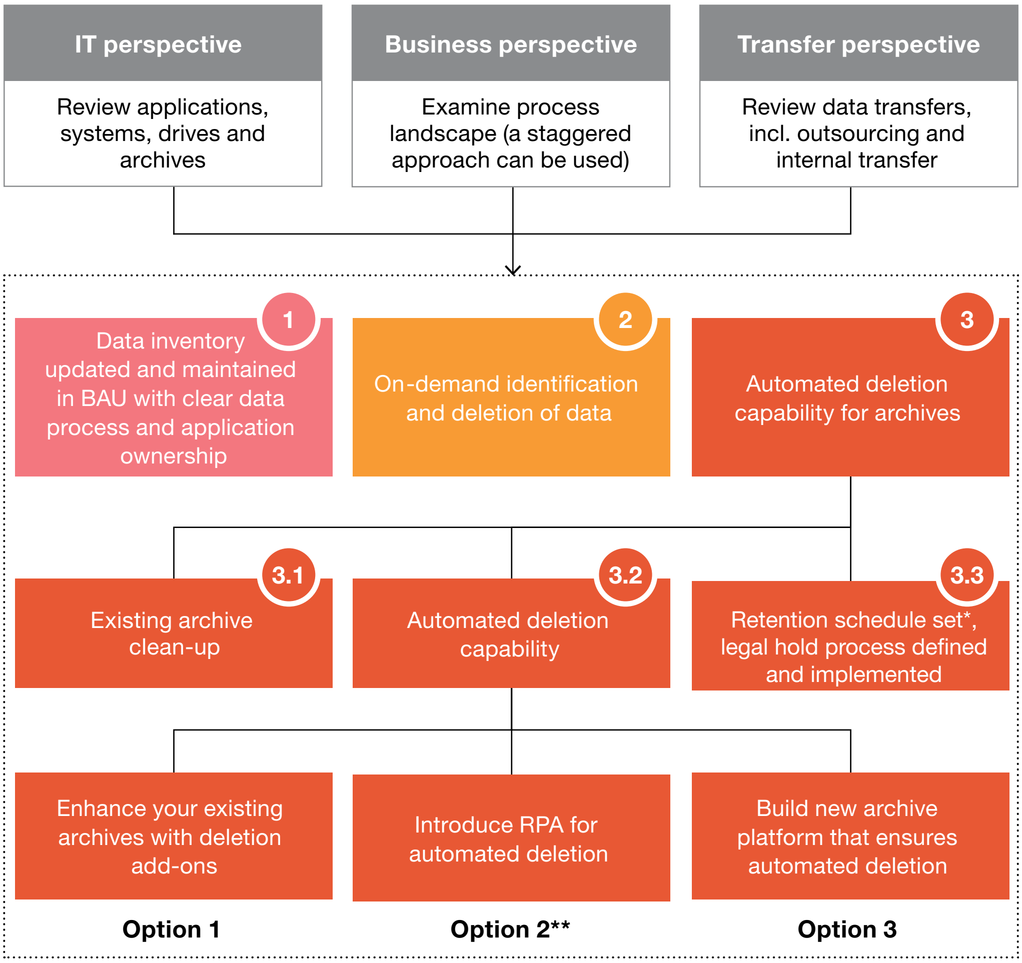
Data protection as a way of enabling the holistic management of structured and unstructured data

To address these regulatory requirements, we would, however, recommend looking at the topic of records and data management not only from a **personal data** perspective, but also from a holistic view of **data management,** as regulatory requirements substantially touch on an operating model's infrastructure.

During EU GDPR implementation program, many organizations have adopted a tactical approach to data identification and deletion and this has already become a major cost driver in business as usual (BAU). Tactical approaches are also subjects to significant risk of not adhering to the regulatory requirements correctly and in a timely manner.

This has shown that strategically answering to the regulatory requirements for records and data management is key to driving cost efficiency in compliance and to enhancing productivity and strategic data based initiatives.

Records and data management framework to ensure compliance with data protection storage limitation and deletion requirements


IT perspective
Review applications, systems, drives and archives
Business perspective
Examine process landscape (a staggered approach can be used)
Transfer perspective
Review data transfers, incl. outsourcing and internal transfer
1
Data inventory updated and maintained in BAU with clear data process and application ownership
2
On-demand identification and deletion of data
3
Automated deletion capability for archives
3.1
Existing archive clean-up
3.2
Automated deletion capability
3.3
Retention schedule set*, legal hold process defined and implemented
Enhance your existing archives with deletion add-ons
Introduce RPA for automated deletion
Build new archive platform that ensures automated deletion
Option 1
Option 2**
Option 3

*incl. other regulatory requirements e.g. Tax/AML etc.

**RPA is normally the least applicable real-life option, given how dynamic business archive systems can be. However, a cost-efficiency case can be made for the use of RPA on archives that are old, not dynamic and, in general, not subject to change. To understand whether RPA could be efficient for your business, you should start by analysing the archives that are in place, their use, and the quality of the archived documentation and the respective metadata. This assessment is a prerequisite for determining the best option and making sure that you opt for the most cost-efficient solution on the basis of your existing infrastructure.

How do you start the records and data management journey in relation to deletion capabilities

Staggered approach from the identification of the scope of your application and system landscape to the final roll-out of your capabilities.

Phase 1
Identify the scope

- Ensure data owners, application owners and process owners are defined incl. roles and responsibilities
- Identify applications, systems, and drives that collect and process personal data (operational applications, with and without storage capability)
- Identify processes where personal data is processed
- Identify storage and archives where personal (structured and unstructured) data is stored
- In particular, the following should be analysed: archive systems (digital archives in a first wave and physical in a second) and back-up systems, temporary recovery systems, etc.

Phase 2
Define requirements

- Define framework for data inventory incl. processes and procedures to maintain in BAU
- Decide on automated deletion capability for archives, i.e. upgrade vs Robotic Process Automation (RPA) vs add-on
- Define framework for on-demand identification and deletion
- Outline a reporting framework for authorities and data subject requests

Phase 3
Build and roll out

- Define functional requirements for automated deletion capability for archives
- Delineate functional requirements for the retention of data
- Roll-out on-demand identification and deletion capability
- Outline measures for data security in processes, applications, other systems and drives

Goal of the analyses in phases 1 and 2

1. Identify – according to application – the need to implement deletion rules based on a pre-defined deletion concept
2. Identify dependencies with third-party application providers and define a roadmap for adoption of deletion capability
3. Define scenarios for the roll-out of the implementation concept on core applications
4. Design a proof of concept (PoC) based on one application
5. Define a process for data clean-up on physical archives
6. Define a process and procedure for handling unstructured data

Challenges observed in the market

1. Today, many organisations lack an overarching view of their application architecture and of how the different applications communicate and exchange data with each other.

2. Often, a clear-cut view is missing of which applications have either or both saving and archiving capabilities. A housekeeping exercise is often required before an organisation can initiate phase 1 of the proposed approach.

3. Major dependency on third-party applications may result in the application owners having limited ability to assess what is necessary to build deletion capabilities. Where this is the case, early alignment with third-party providers is the key to successfully building deletion capabilities.

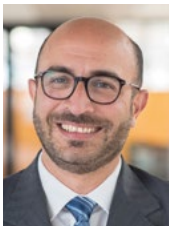
Are you equipped to manage your records and data in the ever-evolving regulatory environment?

How can PwC support you?

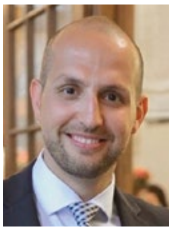
PwC is best suited to support you on your journey to compliance – from a readiness assessment to the implementation of required actions and the basis of your records and data management framework. If your systems are not extremely dynamic, we can support you with RPA implementation. We can work simultaneously with several RPA vendors, allowing separate business units within a company to customise solutions, rapidly digitise processes and deliver significant and sustainable value within short timeframes while reducing overall risks.

For more information please contact:

Regulatory and Transformation



Patrick Akiki
Partner, Finance Risk and
Regulatory Transformation
+41 79 708 11 07
akiki.patrick@ch.pwc.com



Morris Naqib
Senior Manager, Finance
Risk and Regulatory
Transformation
+41 79 902 31 45
morris.naqib@ch.pwc.com

Legal

Yari Iannelli
Assistant Manager, Legal FS
Regulatory and Compliance
Services
+41 79 742 39 04
yari.iannelli@ch.pwc.com

Forensic and Digital Transformation

Angela Carpintieri
Director, Forensic and
Digital Transformation
+41 79 878 31 74
angela.carpintieri@ch.pwc.com

Intelligent Automation

Florian Estoppey
Senior Manager, Artificial
Intelligence and Automation
+41 79 150 25 53
florian.estoppey@ch.pwc.com

Gabriel Jufer
Manager, Artificial Intelligence and
Automation
+41 79 738 99 55
gabriel.jufer@ch.pwc.com

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