



Information Lifecycle Management

Information Lifecycle Management Capabilities for Data Protection and Privacy

A Guide for Customers

Table of Contents

3 Data Protection and Privacy and the Role of SAP Solutions

3 Purpose of This Document

4 The Capabilities of SAP Information Lifecycle Management

5 Why Blocking and Deletion Are Necessary

5 Functionality in SAP NetWeaver for Data Protection and Privacy

6 Functionality in SAP ILM for Data Protection and Privacy

7 Getting Started with Blocking and Deletion

7 Preparation Steps

10 Configuration Steps

11 Execution Steps

12 License Conditions

13 Additional Information, Training, Services, and Assistance

Legal Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP's strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, and shall have no liability for damages of any kind, including without limitation direct, special, indirect, or consequential damages that may result from the use of this document. This limitation shall not apply in cases of intent or gross negligence. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Note: The information contained in this presentation is for general guidance only and provided on the understanding that SAP is not herein engaged in rendering legal advice. As such, it should not be used as a substitute for legal consultation. SAP SE accepts no liability for any actions taken as response hereto. It is the customer's responsibility to adopt measures that the customer deems appropriate to achieve GDPR compliance.

Data Protection and Privacy and the Role of SAP® Solutions

Data protection and privacy (DPP) are critical aspects of digital transformation, and this is recognized through the evolution of numerous regulations demanding increasing data compliance capabilities. For example, the European Union's General Data Protection Regulation (GDPR) introduces "the right to be forgotten," which involves multiple steps in an ERP application, as well as consideration of other legal requirements that may prevent or delay data from being deleted.

The SAP® Information Lifecycle Management (SAP ILM) component provides a broad range of advanced capabilities, including blocking and deletion, residence and retention management, consolidation of legacy data, and more – some of which are relevant to regulatory demands.

Recognizing that blocking and deletion of personal data have become key requirements of many regulations, SAP has included relevant capabilities from SAP ILM as part of the standard SAP NetWeaver® technology platform. Together with other capabilities already available in the standard platform, this helps customers running SAP Business Suite software and SAP S/4HANA® achieve their DPP objectives.

SAP Information Lifecycle Management remains a separately licensed product for additional capabilities and management of other types of data.

PURPOSE OF THIS DOCUMENT

This document is intended as a short guide to information lifecycle management and the capabilities available in SAP NetWeaver to help customers with DPP regulations such as GDPR (among others). It does not cover all the requirements of such broad regulations. Instead, the focus is on blocking and deletion functionality made available to SAP Business Suite and SAP S/4HANA customers, discussing both technical considerations and business decisions. Links provide access to more detailed documentation and reference materials as well as relevant training and services offerings that can assist with implementation projects. The document makes clear what is included in SAP NetWeaver and what is part of SAP ILM as a licensed product.

The Capabilities of SAP Information Lifecycle Management

SAP Information Lifecycle Management plays a key role in managing the context and locality of data during its use within important business processes. This includes archiving data that is not frequently used and managing the retention and then later the responsible destruction of obsolete data based on rules. SAP ILM enables data in legacy systems to be consolidated, managed, and reported on within a single repository, thus allowing legacy systems to be decommissioned, resulting in a simpler landscape and lower total cost of ownership (TCO). Together with its legal-hold capabilities as well as the ability to support e-discovery, SAP ILM is a powerful solution that can help with the data compliance requirements of many regulations, including data privacy and protection.

Archiving	Retention management	Retention warehouse
<ul style="list-style-type: none"> • Control data growth proactively to meet service-level requests • Analyze data volumes • Move data securely from the database to the archive 	<ul style="list-style-type: none"> • Enforce data retention periods required by regulations and industry practice • Manage the responsible destruction of data based on policies • Store data securely with SAP or partner products • Perform e-discovery operations and set legal holds 	<ul style="list-style-type: none"> • Consolidate data from multiple systems • Decommission legacy systems • Run reports on data from decommissioned systems
Data volume	End-of-life data	End-of-life system

Archiving enables you to manage data volume. It helps you keep SAP software systems at optimum operational size by moving less current data into archive files with an automated and governed process.

Retention management helps you manage the lifecycle of the data from its creation to its destruction within a live application system. This includes capabilities for blocking and deletion (discussed later in this document). This capability allows e-discovery to locate information needed to answer legal and similar inquiries together

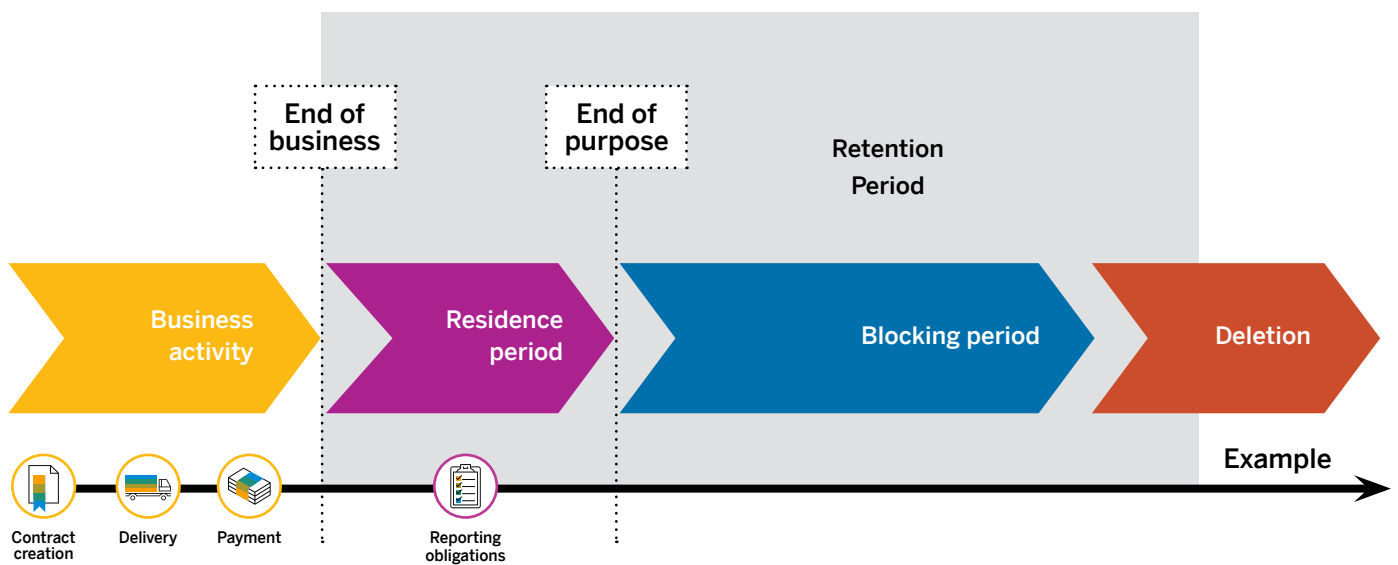
with legal hold to prevent documents that are relevant for legal cases from being deleted or destroyed, whether they are in the database or archived.

Retention warehouse enables the extraction and consolidation of data from multiple systems (SAP and third party) into a single store and provides necessary reporting capabilities. This helps achieve landscape harmonization and simplification as well as significant TCO savings through decommissioning legacy systems and reducing compliance effort and risk.

WHY BLOCKING AND DELETION ARE NECESSARY

Data privacy and protection regulations often require that personal information be deleted at the end of its business purpose or if an individual has requested erasure (right to be forgotten). However, this data may need to be retained longer depending on other laws. SAP ILM allows you to block that data from regular business use while it remains accessible to authorized users for statutory reporting purposes (see Figure 1).

Figure 1: Retention, Blocking, and Deletion



FUNCTIONALITY IN SAP NETWEAVER FOR DATA PROTECTION AND PRIVACY

To help customers meet their DPP objectives, certain capabilities that were previously included in SAP ILM are now included in SAP NetWeaver under certain conditions: these capabilities are to be used for management of personal data only.

Three important features in standard SAP NetWeaver can help customers with DPP initiatives.

Information retrieval framework (IRF) can be used to search for and retrieve all personal data of a specified data subject. The search results are displayed in a comprehensive and structured list

containing not only the personal data but the purpose for which the data was collected and processed.

Read access logging (RAL) can be used to monitor and log access to personal data. The information provided may include, for example, which business users accessed what personal data and when.

Blocking and deleting personal data is done in a structured and integrated manner based on specific rules. Previously available only as part of the licensed SAP ILM component, it is now included in SAP NetWeaver to complement IRF and RAL.

The remainder of this document discusses why blocking and deletion are necessary for DPP purposes and the steps you can take to set this up.

Note: The “License Conditions” section describes in more detail what is provided in SAP NetWeaver and under what conditions and then what additional capabilities are provided by SAP ILM as a separately licensed product.

FUNCTIONALITY IN SAP ILM FOR DATA PROTECTION AND PRIVACY

As a separately licensed product, SAP ILM provides capabilities in addition to those now included in SAP NetWeaver.

Blocking and Deletion for All Kinds of Data Beyond DPP Purposes

There may be additional legal, business, or contractual reasons why other types of data, not just personal data, could and should be deleted after certain periods of time, for example, end-of-life products outside of warranty periods. In this case, companies can use SAP ILM to automate the retention and later deletion of that data while helping to ensure overall consistency across the application landscape.

Data Controller Rule Framework

Managing the automated retention and deletion of data requires the definition of specific rules. The number of rules depends on the variety of different information objects to be managed, combined with the various retention periods stipulated by many legal and business requirements, and considering the organizational structure of the enterprise, which may include multiple subsidiaries, countries, and jurisdictions.

The data controller rule framework reduces the maintenance effort by providing more automated methods to define the multiple rules that are required. In addition, it allows the definition of the different purposes for which such information is being stored, which is an important consideration in many DPP regulations.

System Decommissioning

By consolidating data from legacy systems into a single store, but with required (periodic or ad hoc) business reporting still available on that data, the legacy systems can be decommissioned. As part of SAP ILM, the legacy extract workbench, along with other tools, helps you migrate data more easily into a retention warehouse. This applies whether the legacy systems are older SAP software installations or third-party applications. Then, accelerated reporting together with business user reporting are available to enable business use of the consolidated data.

Simplifying and consolidating the application landscape may be an important step to digital transformation, such as migrating to SAP S/4HANA. With each legacy system that is decommissioned, significant TCO savings can be realized: freeing up physical space in a data center; reducing hardware; eliminating operating systems, databases, and application licenses; and lowering staff costs. Further, shutting down legacy systems can also reduce compliance risks and associated costs.

Getting Started with Blocking and Deletion

The table summarizes steps that are described in the following sections.

Prepare	Configure	Execute
<ol style="list-style-type: none"> 1. SAP NetWeaver® versions 2. External storage requirements (if needed) 3. ILM business functions 4. Application versions and module-specific business functions 5. Business guidance on information residence and retention times 	<ol style="list-style-type: none"> 6. ILM audit area 7. Application and module-specific settings 8. ILM policies, rule groups, and object groups 9. External storage 	<ol style="list-style-type: none"> 10. Initialization and migration runs 11. Blocking runs 12. Archiving runs 13. Destruction runs

PREPARATION STEPS

Step 1: SAP NetWeaver versions

The functionality necessary to support blocking and deletion is available in SAP NetWeaver.

SAP product	SAP NetWeaver®
Software component	SAP_BASIS
Minimum release	SAP NetWeaver 731 – required for ILM
Recommended release	SAP NetWeaver 740 SP13 – required for blocking and deletion

ILM features delivered in each of these releases are listed below.

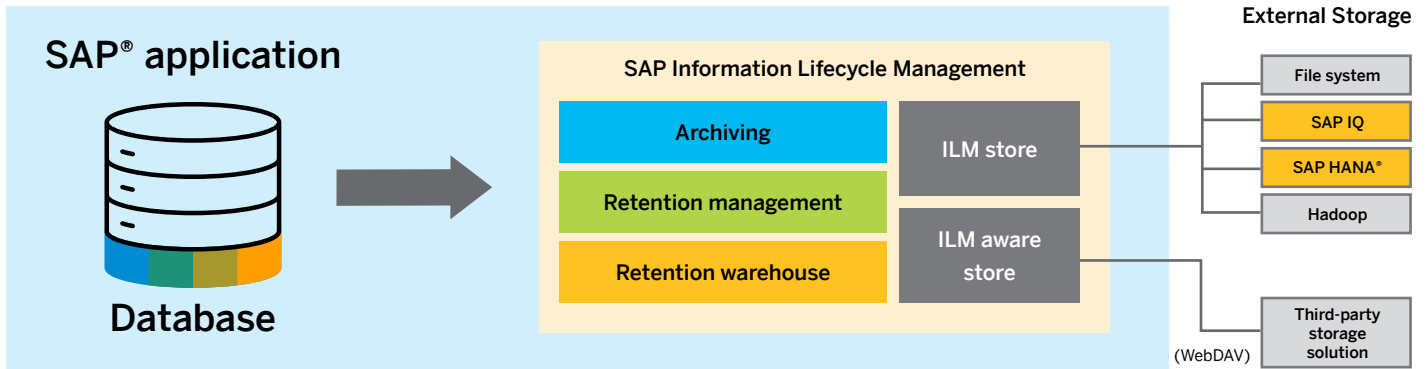
Release	Feature
SAP® ERP 6 (minimum required)	ILM basic features
SAP ERP 6 EHP7 (recommended)	ILM advanced features
SAP_BASIS 740 SP13	ILM store
SAP_BASIS 740 SP12	ILM blocking

Step 2: External storage requirements

Storage is required when data is moved outside of the SAP application database. This is typically for archiving purposes. Support of SAP ILM for different storage infrastructures has expanded over time. The various options are shown in Figure 2 and fall into two main groups:

- ILM store: available with BASIS 740 SP13, direct support of file system, SAP IQ software (columnar database), SAP HANA® business data platform, and Hadoop
- ILM aware store: uses the WebDAV industry standard integration protocol to connect to third-party storage infrastructures ([list of SAP-certified solutions](#))

Figure 2: ILM Stores



Step 3: ILM business functions

To use the functionality for blocking and deletion, various business functions need to be enabled. These ILM business functions are included in SAP NetWeaver and must be activated for each separate SAP system.

Business function	Description
ILM	Information lifecycle management
ILM_STOR	ILM external storage (see note A)
ILM_BLOCKING	ILM blocking functionality (see note B)
BUPA_ILM_BF	Blocking of business partner
ERP_CVP_ILM1	Blocking of customer or vendor
DA_ARCHOBJ_STANDARD_1, 2, 3, 4, 5	Standardized archiving
Module-specific business functions	Described in "Step 4: Application versions and module-specific functions"

Notes:

- A) If using a third-party storage solution through ILM aware store, there is no need to activate ILM_STOR (see Figure 2).
- B) ILM_BLOCKING is used to limit access to transactional data objects and is implemented by moving those to the archive. Business partner, customer, and vendor objects contain personal data, and access can be limited directly in the database by enabling the additional business functions described in the table (termed "Simplified Blocking and Deletion").

Step 4: Application versions and module-specific functions

Each SAP application uses blocking and deletion functionality according to the requirements necessary for the business processes they support. Therefore, it is important to verify the correct version of the SAP application and to configure the relevant module-specific business functions within that application.

The table summarizes relevant version information for a selection of SAP applications.

SAP® application: Minimum recommended version using simplified blocking and deletion	SAP Notes
SAP ERP 6.0 EHP7 SP12	
SAP Supplier Relationship Management 7.03 EHP3 SP05	2011539
SAP Customer Relationship Management 7.0 EHP3 SP05	2039738
IS-UT EHP7	2591185
SAP ERP Human Capital Management 6.0 EHP6 SP16	1559133

For a complete list of applications, versions, and required steps, please refer to the following SAP Notes:

- [1825544](#) – Simplified Deletion and Blocking of Personal Data in SAP Business Suite
- [1825608](#) – Simplified Blocking and Deletion of Central Business Partner
- [2122906](#) – ILM: List of ILM objects with assigned archiving/data destruction objects
- [2590321](#) – Upgrade recommendations to support GDPR compliance

Step 5: Business guidance on information residence and retention times

Blocking and deletion operations have a close relationship with the lifecycle of information, and this is determined by residence and retention times. You need to engage with relevant business stakeholders to understand their requirements for the different kinds of information you will process:

- **Residence time** – How long information is needed for each business purpose and is to be retained in the database before being considered for archiving (transactional information) or blocking (business partner, customer, or vendor)
- **Retention time** – How long information needs to be kept to comply with regulations or business requirements before it can be responsibly destroyed

As an example of retention time considerations, invoices must be retained for tax purposes. In one country, the law may require they be kept for 10 years. In another country, it may be 15 years. You have to configure retention periods for different kinds of information, in different countries, and for different regulations.

CONFIGURATION STEPS

Step 6: ILM audit area

This configures a logical group of ILM objects relative to a business topic or function. For example, when considering what information must be preserved to comply with tax legislation, the relevant ILM objects can be grouped into an audit area named "Tax." Similarly, an audit area named "Product Liability" could be configured to include all ILM objects that relate to the information your business decides must be retained to satisfy any future warranty claims, product recalls, and so on.

Step 7: Application and module-specific settings

The checks to ensure that all prerequisite criteria have been met for blocking business partner, customer, and vendor information are very comprehensive both within and between application modules. To improve performance for large numbers of data objects and provide other supporting functionality, some modules require additional settings. These are described in the SAP Notes listed previously.

Step 8: ILM policies, rule groups, and object groups

Businesses operate by processing many different types of information. It should be clear that not all information can be kept forever nor can it be deleted without considering wider legal and business requirements. The various rules that describe these constraints are defined by policies configured within ILM. Rule groups and object groups, which are collections of ILM objects, simplify the description and maintenance of these policies.

Step 9: External storage

External storage is necessary to support archiving of data. Various external storage options have been described previously and range from a basic file system approach to certified third-party storage systems. These need to be configured according to the relevant documentation for those systems. (See documentation listed in the section "Additional Information, Training, Services, and Assistance.")



EXECUTION STEPS

Step 10: Initialization and migration runs

To ensure optimal performance for blocking (and possible later deletion) of business partner, customer, and vendor information, you must run reports that gather data about the latest closed transactions belonging to those entities. For any information that has already been archived, you should run reports against the archive to determine the latest closed transactions that may belong to those entities.

Step 11: Blocking runs

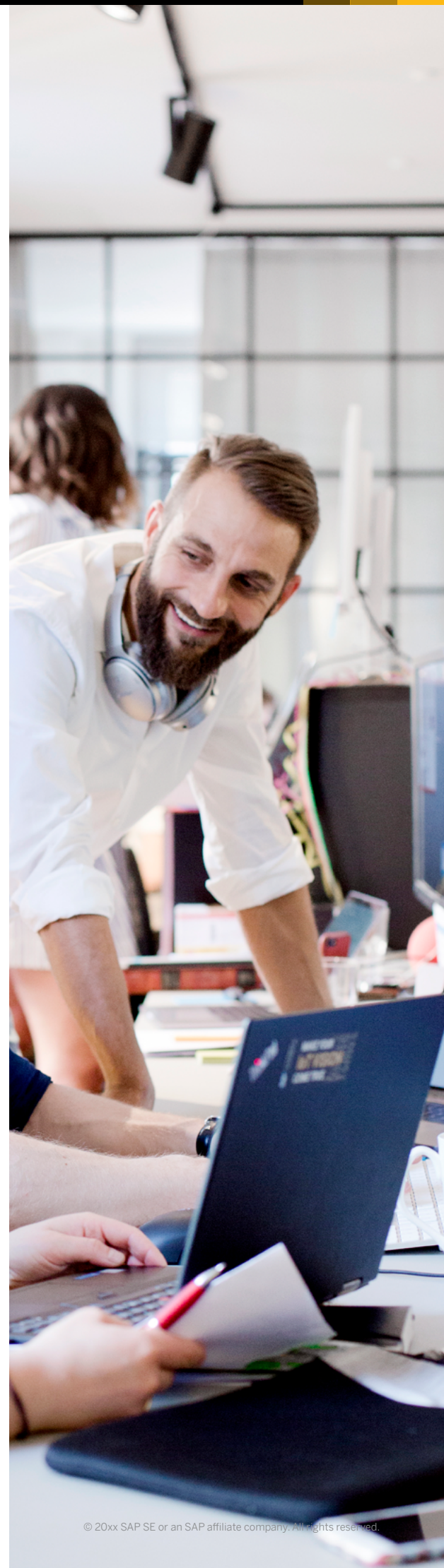
Jobs that check residence times and enforce blocking must be scheduled to run on a regular basis. Once the customers, vendors, or business partners are blocked, no updates or postings should be possible, and access to the data is restricted.

Step 12: Archiving runs

Data that is no longer required for active business purposes and does not need to be maintained in the primary database of the production system can be archived to external storage. Users with appropriate access privileges can still view and query archived data.

Step 13: Destruction runs

Data that is no longer required for business purposes or to meet (potentially) multiple regulatory requirements can be deleted. Data destruction runs can be organized on an initial and ongoing basis. The initial data destruction run may apply when the ILM system is first configured and it is apparent there is a lot of data outside of any retention rules that does not need to be saved or archived, so it can be deleted immediately. Data destruction runs manage the deletion of data according to the retention rules in the configured ILM policies.



License Conditions

Included in the SAP NetWeaver license for GDPR and similar data privacy regulations:

- For all types of data:
 - Data archiving
 - Information retrieval framework
- For personal data applicable to GDPR and similar data privacy regulations:
 - Definition and management of retention policies
 - Storage and retention of information to file system, Hadoop, SAP HANA, and SAP IQ
 - Simplified blocking and deletion of information
 - Destruction of information from archive or database
 - Legal hold including support of e-discovery

Available in SAP Information Lifecycle Management, a fully licensed product:

- Use of ILM, which requires an SAP NetWeaver license that provides the functionality described above, but now extends this to cover all types of data, not just personal data
- Data controller rule framework for automating the definition of multiple retention rules
- System decommissioning to consolidate legacy system information into a single retention warehouse for ongoing reporting requirements and allowing the legacy systems to be retired

- Restricted runtime license of four cores of SAP IQ to provide a fast columnar-storage database to be used solely as a data store for SAP ILM
- Restricted runtime license of SAP Landscape Transformation Replication Server allowing the replication of information between environments to be used only in conjunction with SAP ILM

The license for SAP ILM is applied per managed system. Managed systems are all systems with a unique system ID that are controlled, managed, monitored, or retired by the software. For SAP ILM, only productive-use managed systems are counted. This means that the software can be used in development and test configurations and those system IDs will not count toward the overall license.

Other components relevant to SAP ILM that may require a license:

- The managed systems (as defined above) have their own independent license requirements whether those are from SAP or other business application vendors.
- The platforms that provide capability as data stores for ILM may have independent license requirements whether these are provided by SAP or third-party vendors.

Additional Information, Training, Services, and Assistance

DOCUMENTATION

- [Product documentation for SAP ILM](#)
- [Product documentation covering data protection for cross-applications](#)
- [Configuration, installation, and upgrade guides for SAP ILM](#)

TRAINING AND EDUCATION

Courses for data archiving and information lifecycle management are available [on the training Web site](#).

- [BIT660](#) – Data Archiving
- [BIT665](#) – SAP Information Lifecycle Management
- [BIT670](#) – ILM/data archiving – customer-specific development (available only in Germany)

SERVICES

Implementation service for SAP Information Lifecycle Management and implementation service for SAP ILM retention management (for data protection and privacy)

The following consulting services are available for SAP ILM:

- **Scoping workshop:**
 - Introduction to SAP ILM, data protection, and privacy
 - Introduction to simplified blocking and deletion of business partner, employee, customer, and vendor information
 - Review of archiving and retention strategy and scope verification

- **Analysis service:**

- Analysis of production system for simplified blocking and deletion of business partner, employee, customer, and vendor information
- Definition of prerequisites and best-practice recommendation for future implementation

- **Proof of concept:**

- Demonstration of end-to-end scenario based on a predefined scope
- Conducted in a sandbox environment

- **Implementation service:**

- Complete implementation of simplified blocking and deletion of business partner, employee, customer, and vendor information according to customer requirements
- Conducted in a production environment

Additional information on services is available in the solution brief "[Implementing Information Lifecycle Management to Meet Business Needs](#)."

TECHNICAL ASSISTANCE

To report incidents or for technical assistance, please contact a support representative with queries logged under component BC-ILM* or find more information by using the [SAP Support Portal](#) service.

CONTACTS

For more information or to request nontechnical assistance, please use one of the support paths listed [here](#).

Follow us



www.sap.com/contactsap

Studio SAP | 58152enUS (18/05)

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See www.sap.com/corporate-en/legal/copyright/index.epx for additional trademark information and notices.

THE BEST RUN

