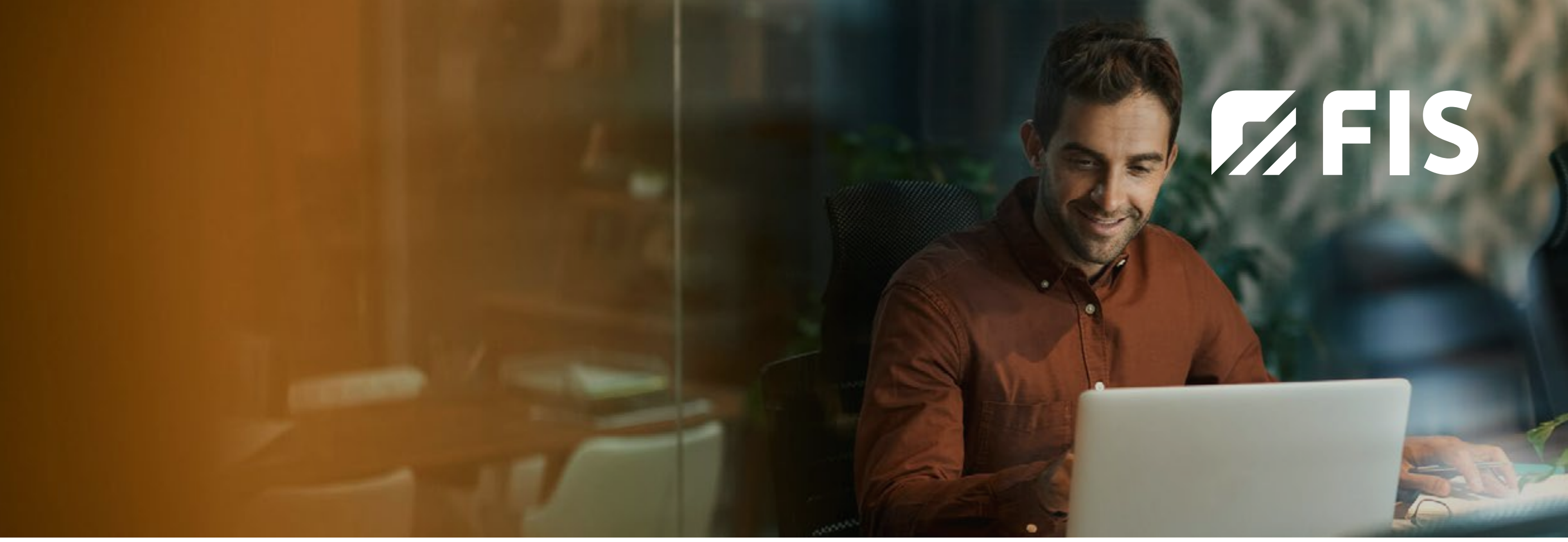

Handle personnel data in compliance with data protection requirements

WITH THE FIS/HRD CCC DATA INFORMATION ANALYSIS

In an HCM system, the amount of personal data that needs to be protected is particularly high. For GDPR-compliant data retention in SAP HCM and SAP H4S4, SAP offers the SAP Information Lifecycle Management (SAP ILM) component, an optimal solution for secure storage and the continuous cleansing of sensitive data. For this purpose, an individual lock and deletion concept is used.

For the initial setup and definition of a lock and deletion concept with SAP ILM, a comprehensive analysis of the current data basis is necessary at first. The analysis must determine all personal data in the SAP HCM system. It is also important to determine the relevance of this data. This gives you system-supported full transparency about the data worthy of protection in your HCM system and how it is used.

Your Benefits

- ✓ GDPR-compliant handling of your personnel data
- ✓ Efficient analysis of datasets for GDPR-compliant operation of your HCM or H4S4 system
- ✓ Provision of data for the continuous optimization of the lock and deletion concept
- ✓ Determination of person-related entries in upstream systems for cross-system security

Analyze data worthy of protection in the SAP HCM and H4S4 system

As part of an ILM project, it is determined which data may be retained in the SAP system for how long and after what period of time it is deleted. As a basis for defining these rules, the FIS/hrd CCC DIA tool determines at various depths of analysis which personal data is available and how long this data has existed in the system. As the relevance of the data is crucial for GDPR-compliant data retention, the application also determines whether and when the data was last accessed or changed.

The data information analysis of FIS/hrd CCC examines not only the production systems but also the development and test systems. These upstream systems are often forgotten when creating lock and deletion concepts, but usually also contain data worthy of protection. Due to the irregular use of data in the upstream systems and the authorizations, which are often more extensive, special attention must be paid to the existing datasets in development and test systems.

Based on the comprehensive analysis with FIS/hrd CCC DIA, you can quickly and reliably define an efficient lock and deletion concept. Based on this concept, the corresponding deletion rules in the ILM system can be directly created.

FIS/hrd CCC

(Copy and comparison tool)

- **Data protection:** only anonymized data outside the production system
- **Security:** tests and comparisons can easily be made
- **Time saving:** support for trouble-shooting and mass data tests
- **Flexibility:** individually configurable via separate Customizing

DIA component
(Data Information Analysis)
GDPR compliance and data protection

FIS/hrd SRA

(Schema and Rule Analyzer)

- **Audit compliance:** versioning of "schemas & rules"
- **Traceability:** easy and fast documentation in the system
- **Transparency:** comprehensive comparisons within and between systems
- **Always up to date:** support for the import of support packages

ORC component
(Operational Relevance Check)
Lean system, no obsolete data

The data information analysis by FIS/hrd CCC is part of the FIS/hrd tool set

Optimized Information Lifecycle Management through continuous monitoring

The initial implementation of the lock and deletion concept alone cannot permanently ensure GDPR-compliant data retention. Company-specific extensions to the data records, changes to access authorizations and links or an adaptation of the SAP standard version require constant further development of the ILM.

Change requests to the ILM cannot always be recognized directly by the users. By regularly checking the dataset in your system using FIS/hrd CCC DIA, you can determine at any time whether data records have been in the system longer than required or permitted or whether new personal data has been stored in tables that have not yet been viewed. This information can be used to adapt the existing lock and deletion concept and ensure a permanent GDPR-compliant data retention.

Securely positioned with FIS/hrd CCC DIA

The DIA component of FIS/hrd CCC supports the design of a lock and deletion concept by analyzing the dataset in your system on a field and usage basis. Regular monitoring of the data worthy of protection in your SAP HCM or H4S4 system ensures that data retention permanently complies with the defined rules and facilitates the continuous optimization of the concept.

In this way, you save time and effort for GDPR-compliant cross-system data retention. In addition, you gain security with regard to the correct configuration of the Information Lifecycle Management in your systems.

FIS Informationssysteme und Consulting GmbH
Röthleiner Weg 1
D-97506 Grafenrheinfeld
info@fis-gmbh.de
www.fis-gmbh.de/en