



Do you know where your most important sensitive company data is saved? Only those who know where the sensitive data in a company is located can store it appropriately and protect it in line with legal requirements. Identifying sensitive data is therefore becoming increasingly important.

**Sensitive Data Services identifies and categorises the most important sensitive data in your organisation.**

**What is Sensitive Data Services?**

Sensitive Data Services is a Managed Service that uses the DataScout software solution to create a data inventory of all stored data in your company. This inventory shows where the data is located, the related data categories and how much sensitive data is present in your organisation. This overview serves as the basis for further projects, such as regulatory (GDPR) compliance, preparation for migration to the cloud or protection against data loss and cyber attacks.

**Benefits of Sensitive Data Services**

- Your stored data (structured as well as non-structured data) will be analysed.
- Your data will not be copied and will never leave your company.
- Your sensitive data is categorised and summarised in a statistical report.
- Sensitive Data Services can be easily adapted to your individual business needs and supplemented with additional Swisscom services (Audit Guard and Data Loss Prevention for example).
- You receive a comprehensive and professional Managed Service that can be implemented within a short time and with minimal technical requirements.

**How Sensitive Data Services works**



**Data Profiling**  
Identify where potential sensitive data is stored



**Data Category Matching**  
Crawl all data sets and match these against pre-defined categories



**Exact Data Matching**  
Verify matches against real data-sets (Fingerprinting)



**Reporting**  
Provide statistical reports on matched data categories



## Facts & figures

 <b>Basic services</b>	Installation and maintenance of the DataScout software solution
	Integration into the existing IT infrastructure
	Definition and implementation of customer-specific data categories (search patterns)
	Statistical reports for each scanned data repository
	End-to-end service performance from the query to the final report
 <b>Optional services</b>	Data anonymisation (e.g. for test environments)
	Exact data matching: any algorithm-based data consistencies that are identified are compared with the currently known data from your company (e.g. customer data). Hashed indexes are created for this purpose.
	Whitelisting of specific data (e.g. employees)
	Scanning by specific document types (e.g. customer contracts, patent applications, application documentation or employment contracts)
	Automatic assignment of document types to appropriate data repositories (e.g. Strictly Confidential, Internal, Public)
 <b>Additional services</b>	Logging of all activities related to sensitive data and reporting of any violations of industry-specific standards (Audit Guard)
	Data loss prevention (to prevent the loss of sensitive data)
	Advice on regulatory compliance (GDPR, FINMA etc.)
	Preparation of data repositories for easier migration to the cloud

The information in this document does not constitute a binding offer. It is subject to revision at any time.

Swisscom (Switzerland) Ltd Enterprise Customers, P.O. Box,  
CH-3050 Berne, Telephone 0800 800 900, [www.swisscom.ch/enterprise](http://www.swisscom.ch/enterprise)