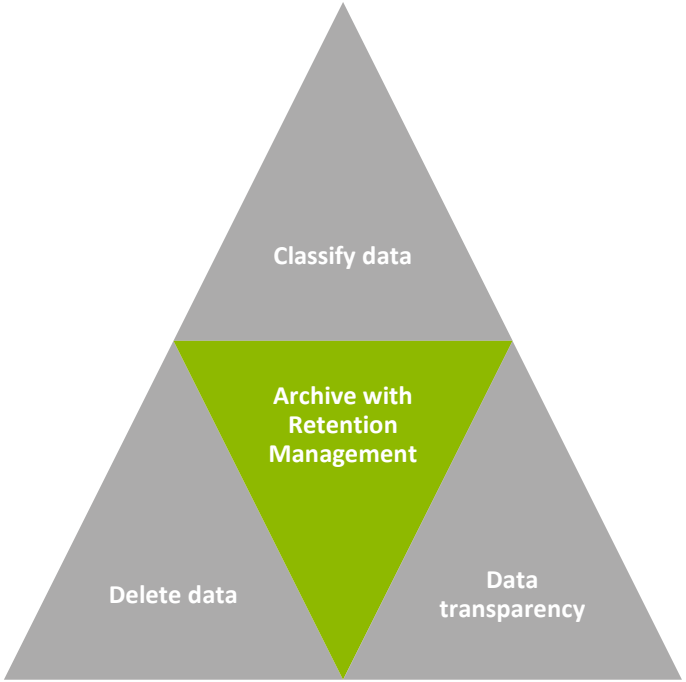
How does iCAS specifically meet the requirements of the GDPR?

GDPR & Software-Defined Archiving

- Privacy-focused archiving provides the foundation for GDPR-compliance
- Many requirements of the GDPR are easier to implement based on a central data management with retention management
- Software-defined systems facilitate participation in technological development



Overview: GDPR requirements & iCAS

What the GDPR requires:	How iCAS fulfills these requirements:
▪ §5(1)(c-e-f): Data minimization, storage limitation, integrity and confidentiality	▪ Separation of user- & metadata, WORM, file-based retention, CSC technology, integrity tests, etc.
▪ §15: Right of access by the data subject	▪ Integration in e-discovery & search tools
▪ §17: Right to erasure (Right to be forgotten)	▪ Special delete, legal hold
▪ §24(1): Continuous monitoring of the implemented technical & organizational measures	▪ Monitoring of logging data, audit trail/history
▪ §25: Data protection by design and by default	▪ CSC technology, WORM etc., audited & certified by KPMG
▪ §30: Record of processing activities	▪ Audit trail/history, changelog
▪ §32: Security of processing	▪ Encryption at Rest, high-availability service, Self-Healing
▪ §33 & 34: Data breach	▪ Documentation about all events in the backend

§ 5(1c): Data Minimization

What the GDPR requires:

“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”

Technical requirements:

- Systems may not generate unnecessary duplicates
- Personal user data and metadata must be processed separately

How iCAS fulfills it:

- User and metadata are retained separately
- The separation is fixed in the settings
- No personal data is stored in metadata or combined with it

§ 5(1e): Storage Limitation

What the GDPR requires:

Personal data

…shall be kept for no longer than is necessary;

…may be stored for longer periods solely for certain purposes (e.g. historical research).

Technical requirement:

- Systems must be able to set time limits in storing every data

How iCAS fulfills it:

- WORM-based retention applies a fixed retention period to every file
- Data can be automatically erased when the retention expires
- Very long retention period options exists

§ 5(1f): Integrity and Confidentiality

What the GDPR requires:

"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage."

Technical requirements:

- Systems must have access control to prevent data modification
- Systems must ensure accurate and complete data transfer to storage
- Systems must be able to detect corrupted/ invalid data and repair it

How iCAS fulfills it:

- CSC technology encapsulates data that can only be accessed via an associated key
- Optional encryption at rest
- Check mechanisms (Read-After-Write and Verify) ensure accurate and complete data transfer to the storage solution
- Regular data integrity checks (corrupted data will be replaced with valid data thanks to the Self-Healing functionality)

§ 15: Right of Access by the Data Subject

What the GDPR requires:

Data subjects have the right to obtain confirmation if their personal data are processed and, if this is the case, obtain access to their data and some other information.

Technical requirement:

- Systems must be able to locate and retrieve all archived data without delay

How iCAS fulfills it:

- Centralized data storage/central archive storage platform simplifies data search
- Integration in e-discovery and search tools
- Validated for 120+ leading business applications

§ 17: Right to Erasure/to be Forgotten

What the GDPR requires:

Under certain circumstances, data subjects have the right to request erasure of their personal data...unless in special cases (e.g. legal claims).

Technical requirements:

- Systems must be able to erase data and its copy without delay before the defined retention period expires
- Systems must be able to keep data even after the retention period expires

How iCAS fulfills it:

- Special Delete: Erase archive data before the originally defined retention period (special and correctly-defined process)
- Legal Hold: Retention periods can be extended with iCAS

§ 24(1): Responsibility of the Controller

What the GDPR requires:

…to ensure and to be able to demonstrate that data processing (including storage) is performed in accordance with GDPR.

Technical requirement:

- Continuous monitoring of the implemented technical measures

How iCAS fulfills it:

- Monitors logging data (logged access) regularly in a GDPR-compliant manner
- Creates a documentation and archives it in an audit-compliant manner
- Protects the documentation against changes
- Audit Trail/History: records all actions undertaken (e.g. attempts to erase, change of logs)

§ 25: Data Protection by Design & Default (I)

What the GDPR requires:

…to implement data protection principles, both when determining the means for processing and during the processing itself…

Technical requirements:

- Systems must be designed to protect data and to integrate necessary safeguards into data processing (incl. storage)
- By default, systems must process only necessary personal data (amount, extent, storage period, accessibility)

How iCAS fulfills it:

- iCAS had been audited and certified by KPMG for its ability to meet the GDPR requirements. Find all details in the audit report
- WORM functionality and patented Content Storage Container (CSC) prevent data manipulation and unauthorized deletion
- AES-256 Encryption at Rest: prevents unauthorized access to archive data
- Self-Healing: identifies and repairs damaged archive objects
- Self-Testing: detects and reports potential data corruption (when data redundancy is not desired)
- Further details on the next page…

§ 25: Data Protection by Design & Default (II)

What the GDPR requires:

…to implement data protection principles, both when determining the means for processing and during the processing itself…

Technical requirements:

- Systems must be designed to protect data and to integrate necessary safeguards into data processing (incl. storage)
- By default, systems must process only necessary personal data (amount, extent, storage period, accessibility)

How iCAS fulfills it:

- Provides access only to authorized users
- Documents all attempts to access archive data in audit logs
- Retention management (time stamps & lock): applies a fixed storage period to every file, protects data from deletion before the specified period
- WORM/file-based retention: ensures deletion of data within the specified period
- Multi-tenancy capability: enables a centralized management of archive data, minimizes risks posed by management of many different systems

§ 30: Record of Processing Activities

What the GDPR requires:

…maintain a record contains e.g. general description of the technical measures implemented in security of processing (incl. storage)…

Technical requirement:

- Systems must be able to provide such record automatically

How iCAS fulfills it:

- Audit Trail/History: all events occurred to archive data (e.g. access to CSCs from an application) are documented in a compliant manner
- No personal data is included in the history
- Changelog: records any changes to the configuration of archive data (e.g. activation of Legal Hold)

§ 32: Security of Processing

What the GDPR requires:

…ensure a level of security appropriate to the risk.

Technical requirements:

- Encryption of personal data
- Ongoing integrity and availability of processing systems
- Systems must be able to restore the availability and access to personal data in a timely manner in case of a physical or technical incident

How iCAS fulfills it:

- AES-256 Encryption at Rest for high-level security of the archive
- Provides high-availability services via Microsoft Failover Cluster
- Self-Healing: replicates the archive, identifies & repairs broken objects. Logical/technical failures of System-A can not influence the replicated System-B

§ 33 & 34: Data Breach

What the GDPR requires:

…notify personal data breach to supervisory authority and data subject without undue delay

…document facts relating to data breach…

Technical requirement:

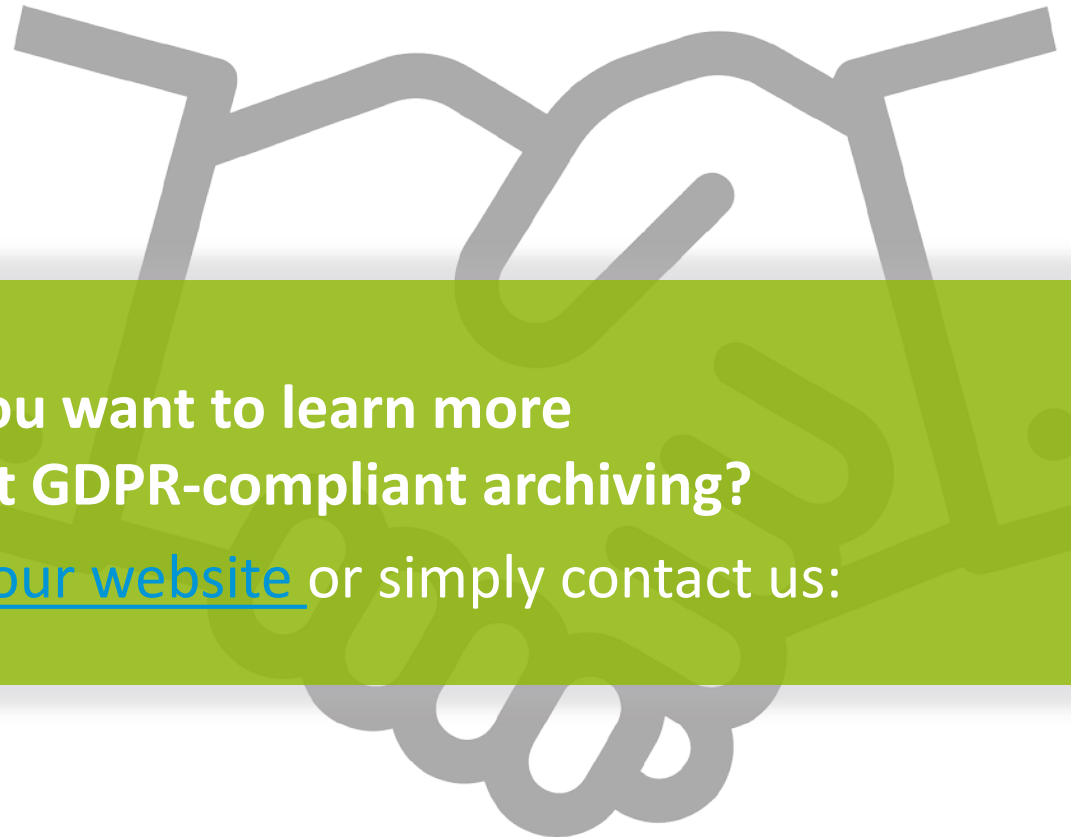
- Systems (incl. storage) must be able to generate the required facts

How iCAS fulfills it:

- Provides controllers with information about data breach that occurs in the backend, e.g. attempts to erase or change of logs (Audit Trail/History, Self-Testing, Changelog)

iTernity GmbH

- Software solution provider for future-proof data management and legally compliant archiving
- iTernity has won multiple awards for its innovative approach to long-term data storage
- Close partnership with leading global IT companies (HPE, Microsoft, …)
- KPMG audited and certified iTernity and iCAS for GDPR-compliance
- 1200+ customers worldwide in all industries rely on iCAS



Do you want to learn more about GDPR-compliant archiving?

Visit our website or simply contact us:

iTernity GmbH
Heinrich-von-Stephan-Str. 21
79100 Freiburg

sales@iternity.com
+49 761 / 590 34 810