Archiving and the GDPR

Information on use of the xSuite Archive in compliance with data protection regulations

November 2022

xSuite Archive

The obligations and sanctions under data protection law have been extended considerably since the GDPR (General Data Protection Regulation) came into force. We, for our part, have therefore worked in great detail with the requirements in order to ensure that our software complies with data protection regulations.

In this document, we offer our prospective customers, and existing customers, and partners an overview of how our software solution xSuite Archive can be used in compliance with data protection regulations. In terms of the legal requirements, we describe which functions and settings are available to you when using the archive.

Please note that the use of the software in accordance with data protection laws is the sole responsibility of the user. In particular, this includes the individual configuration of the software and its functions. The guiding principle in working with the software is that the more sensitive the data, the greater the need for protection of personal data.

The following explanations are offered for informational purposes only. We expressly do not provide any legal advice and therefore do not assume any liability for the following contents.

In case of doubt, we recommend that you seek advice from a lawyer specializing in data protection.

What requirements does the GDPR place on an archive solution?

The right of access by the data subject (Art. 15 GDPR)
As the party responsible, you are obliged to disclose upon request which personal data you are processing regarding an individual, and for what purpose. In order to do so, you must be able to locate personal data quickly, easily, and in its entirety. Personal data can generally be accessed in xSuite Archive on several different levels: xSuite Archive offers full-text search (Google-like search for document content), index field search (search using predefined fields such as editor) and metadata search (search for properties of data and documents, such as „document creator“). Which of these options is available depends on your company‘s configuration.

The right to rectification (Art. 16 GDPR)
As the party responsible, you are obliged to correct any incorrect data concerning a person. It must therefore be possible not only to find the exact piece of data you are searching for, but also to change it. The decisive question here is whether the data is managed in a leading system (e.g., ERP), whether it is managed directly in xSuite Archive or whether it is a mixed form. If the location of the inaccurate data is the ERP system, then the data must be corrected within that system. For data stored in the archive, changes can be made directly in the respective screen. When creating a new version, the previous version of the data will be retained for the purposes of traceability. These are the default settings, and they can be disabled in the configuration if previous versions should not be traced.

The right to erasure (the „right to be forgotten“) (Art. 17 GDPR)
As the party responsible, you are obliged to delete personal data as soon as the intended purpose no longer applies. Furthermore, you may be obliged to delete stored personal data concerning a person, in compliance with his/her request. Once a search has been run, a user with the required authorization can delete the selected data records. It is advisable to proceed selectively and to carry out individual checks, as it is possible that individual documents may not yet be deleted due to ongoing storage obligations. You should check which data and documents are to remain archived.

The right to data portability (Art. 20 GDPR)
According to the GDPR, it must be possible to transfer data records in machine-readable format from one system to another. xSuite Archive provides a function to export all or selected records and documents for purposes such as offline viewing. Documents are exported in the format in which they are saved; the index data is exported as a JSON file. The user can configure the software to allow online access, either to all the contents, or just to certain details.

xSuite Archive as part of an integrated solution
Independent of the standard functions provided by xSuite Archive, the archive should always be seen in the overall context. For instance, one should be aware that deleting data in the archive will not suffice if the archive is downstream from the connected ERP system. Should this be the case, the data will need to be modified or deleted in the ERP system.

Privacy by design — features and options for data protection

xSuite Archive provides a number of features and options to enable or facilitate data protection compliance:

Users, authentication and passwords
- xSuite Archive has authorization management but no user management. User administration and authentication is performed by a service provided by xSuite Core. This means that neither user data nor passwords nor any other user identification features are stored in xSuite Archive.
- xSuite Core, where user authentication is performed, always uses another system such as an active directory. The mechanisms and settings for authentication are applied by way of this system. You can use it to implement password policies according to your company‘s privacy policy.
- The client can only access the system via REST services. These services are hosted in the Microsoft IIS, which is where authentication can be set.
- xSuite Archive is shipped with a default user role password, which can (and should) be changed.

Encryption
- The encryption standard used is AES-256.
- The client only has web access to the system via REST services. These services are hosted in the Microsoft IIS, which is where encryption (HTTPS) can be set.
- Communication can be encrypted end-to-end with an SSL certificate.
- The property “Stream type = Crypted” can be added to the archive. This will automatically encrypt all the documents that are added.
- Only the passwords of back-end users (i.e., services, not human users) are stored in xSuite Archive. A tool is available for encrypting the passwords and credentials of these back-end users. The setting „salted“ also ensures that the hash cannot be traced.

Caching
- The document caching function can be de-activated.
- Passwords are not cached.

Client-enabled
- The solution is client-enabled in order to ensure that users only have access to the data that originates from the business units to which they belong.

Individual assignment of rights
- xSuite Archive ‘s authorization concept is role-based. Rights such as „Read,“ „Write,“ or „Administer“ can be assigned to roles such as „Employee“ or „Freelancer.“ A user can have several roles. If the roles contradict each other, a role prohibiting participation will take precedence over one authorizing it.
- The assignment of rights is set up as restrictively as possible and is similar to that of Linux systems: What is not allowed for the role is not specified, only what is. Therefore, if nothing is defined, the role will have no authorizations.
- In your settings, you can even restrict administrator access to documents. This type of setting is recommended for personal data of particularly sensitive nature — personnel files, for instance.

Logging
- xSuite Archive provides different log levels for changes to documents and error messages from the system. The most superficial level is a recording of the audit trail, and the most detailed level is trace, in which the smallest bits of information are recorded. Logging cannot be completely deactivated, with the effect that changes will not be made unnoticed.
- Automatic versioning and version history are available for tracking of changes in documents. Index fields indicate who has modified a document, and what the modification was.
- Changes made to field contents are also logged.
- Even the deletion of a document by an administrator is logged: record is made of the fact that a document existed, as well as the creator, time of creation, and time of deletion. The contents of the document (which is the only place containing personal data) are not, however, part of the log.
- The logins of users, including backend users, are logged even if no changes have been made.

Hash
- When documents are stored in xSuite Archive, a header is hashed to protect documents in the file system from changes. The files, in turn, are stored in document boxes which also have a hashed header. This doubled hashing indicates when documents have been manipulated, and as such is yet another measure protecting archived data.
- The system can be configured to check the hash each time a document is displayed in the client. Thus, in keeping with maintenance of data integrity, you can always track whether a document has been changed.

Time stamp and version number
- The system ensures that documents cannot be changed simultaneously by two different processes or users. The changes that apply are those made by the processes or users that access the document first. This supports data integrity.

Legal Hold
- A change lock can be set for all users („legal hold"), preventing documents from being changed or deleted.

Replication
- Automatic replication jobs can be scheduled. This creates replicas as local or remote copies, as desired. The replicas receive a change token to ensure that replica and original are identical. It is possible to activate an automatic check of the replicas with the option „Check Replication" to ensure data integrity.

Data backup
- xSuite Archive provides an export interface for data backup. Best practices for data backup are described in the Administrator's Guide.

Retention/ automatic deletion
- Documents can be designated an expiration date. When the expiration date of a document has arrived, the retention function will automatically trigger deletion of the document. This function supports the data-protection requirements for limiting data stored and minimizing data to that which is necessary for the purposes of processing.
- Retention periods can be set differently for different sub-archives. You can also set up a dedicated archive for documents that need to be retained for long periods. If you classify your documents by retention period and separate them into different sub-archives, you can use retention periods to achieve the goal of limiting document retention to the required length of time.

Indexing and retrieval
- In order to comply with the right to be forgotten, you must be able to retrieve documents that contain personal data. xSuite Archive offers extensive indexing and search functions for these purposes.
- Indexing: To retrieve documents, they must be indexed.
- Search options: Our solution provides a wide range of search options for retrieving all personal data from the archive. Search options include full-text search, which is Google-like search for document contents; index-field search, which involves searching through pre-defined fields such as „user"; meta-data search, i.e., searching according to properties of data- and documents such as the creator of a document; Google-like, schema-free search; automatic completion; relations; search by category; and one-click filters.

Reference lists
- In addition to search functions for users, the administrator has the option of creating reference lists. These reference lists can be used to change or delete all data relating to a specific keyword. This function enables you to comply with your obligation to provide information or to correct inaccurate information, as well as your obligation to delete data.

Commissioned data processing and technical-organizational measures at xSuite

Within the scope of project activities and software maintenance, it cannot be ruled out that our employees may come into contact with personal data. For this reason, we keep a pre-filled data processing agreement for you. In addition, we provide you with a document that describes the technical and organizational measures we take at our company to provide data security.

e-xSuite Archive/GDPR. © xSuite Group GmbH 2023. All rights reserved. Subject to change without notice. Error 2xcepted.