

## WhitePaper

# Compliance with the Requirements of GDPdU using the Software GFI MailArchiver 6 for Exchange

compiled in cooperation with



<b>A. Introduction .....</b>	<b>2</b>
<b>B. Legal principles.....</b>	<b>3</b>
<b>C. Technical and organisational requirements .....</b>	<b>4</b>
<b>I. Electronic evaluation .....</b>	<b>4</b>
<b>II. Completeness and unalterability .....</b>	<b>5</b>
<b>III. Secure and traceable data processing and data storage.....</b>	<b>5</b>
<b>IV. Adequate data accessibility .....</b>	<b>5</b>
<b>V. Assignment capability of e-mails and related business transactions.....</b>	<b>6</b>
<b>VI. Provision of adequate process documentation.....</b>	<b>6</b>
<b>VII. Data protection requirements .....</b>	<b>6</b>
<b>D. Risks.....</b>	<b>6</b>
<b>E. GFI MailArchiver 6 Checklist .....</b>	<b>9</b>

## **A. Introduction**

We can no longer imagine conducting business without e-mail. Today entire transactions are conducted based on e-mail exchanges.

As e-mails often serve as business letters and so-called “commercial letters“ and are also significant for taxation, specific requirements regarding processing and retention of these e-mails are imposed.

The German Tax Code (§ 147 AO) controls the requirements for tax-relevant e-mails. Pursuant to the Tax Code, tax-relevant e-mails must be retained for either six or ten years.

In addition, a detailed statutory regulatory requirement on data access of the German fiscal authority called GDPdU (broadly translated as “Generally Accepted Principles of Data Access and Auditability of Digital Documents“) has been in effect in Germany for several years.

According to this regulation, all e-mails with tax-relevant content are to be electronically retained for the duration of the statutory retention period and must be made available on request of the fiscal authorities.

Specific requirements regarding nature, format and processability of electronically retained e-mails must be satisfied.

An arbitrary storage in individual mailboxes of personnel or a printout of tax-relevant e-mails are now insufficient.

Companies that have not adjusted their financial accounting to the new statutory requirements of GDPdU may be subject to substantial sanctions in their next tax audit. Exceptionally severe violations may result in an estimation of the tax basis as well as penalty payments and a fine on arrears that can amount to EUR 250,000.

Electronic archiving systems offer a compliance solution to the high demands of e-mail retention.

Note, however, that a solely technical solution by itself does not lead to compliance.

Compliance with retention requirements can be achieved only through technical solutions in combination with coordinated procedures and processes.

It is a prevalent misapprehension that a “certified“ system by itself suffices to comply with the various requirements. That is simply not true.

Many software producers leave their customers unaware of the true extent of compliance requirements and may conceal that in addition to simple storage, organisational procedures in connection with the filing structure for e-mails and

attachments as well as prompt retrieval must be implemented.

GFI Software strikes a new path. In addition to a certification issued by a German accountancy of the e-mail archiving software GFI MailArchiver 6 concerning compliance with GDPdU, GFI Software offers a comprehensive solution. In addition to the proven technical archiving solution, support for the structuring of the necessary organisational procedures and processes is provided.

This document is designed to provide information about the requirements of German fiscal authorities and to support, on the basis of a pragmatic checklist, the implementation of procedures pursuant to statutes.

## B. Legal principles

Pursuant to German commercial and fiscal law (§§ 238, 239, 257 HGB and §§ 145-147 AO) account books and other accounting records can be maintained under certain conditions on an image carrier or any other data carrier.

Accordingly, storage of tax-relevant documents on digital data carriers – e.g. in electronic archiving systems – is possible. Electronic archiving is defined as unalterable long-term storage of documents subject to retention obligations on machine-readable data carriers to fulfill the statutory retention requirements pursuant to § 257 HGB and 147 AO.

Documents subject to retention obligations are e. g.:

- accounting vouchers, account books and commercial letters
- physical documents in hard copy (e. g. incoming commercial letters or manually generated accounting vouchers and other vouchers)
- procedure documentation and user manual, documentation of the internal control system (ICS) as well as other documents needed for understanding the financial accounting

E-mails with tax-relevant content also fall into the category of documents with a retention obligation pursuant to § 147 (1) No. 5 AO.

Details of the statutory specifications can be gathered from different relevant statements, policies and regulations, including amongst others:

- Grundsätze ordnungsmäßiger Buchführung (GoB, broadly translated as “Generally Accepted Principles of Proper Accounting”) in accordance with §§ 238 *et seq.*, 257 HGB and §§ 147 *et seq.* AO
- Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS, broadly translated as “Generally Accepted Principles of Computer-Assisted Accounting Systems“), issued by the Federal Ministry of Finance (BMF) in a written communication on 7 November 1995

- Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), issued by the BMF in a written communication on 16 July 2001

With an intent to provide details of these requirements, the Institute of German Public Auditors (“Institut der Wirtschaftsprüfer in Deutschland e.V.“, IDW) published on 11 July 2006 a statement for proper accounting when applying electronic archiving, called “Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren“ (IDW RS FAIT 3).

Additionally, there are data protection requirements determined by the Federal Data Protection Act (“Bundesdatenschutzgesetz“, BDSG).

### **C. Technical and organisational requirements**

Regulations, including pronouncements of the German fiscal authorities, do not prescribe any certain technique for electronic archiving. However, there is mutual agreement about certain technical and organisational requirements related to any system for electronic archiving of e-mails:

- electronic evaluation
- completeness and unalterability
- secure and traceable data processing and data storage
- adequate data accessibility

- assignment capability of e-mails and related business transactions
- provision of adequate process documentation
- data protection requirements

### **I. Electronic evaluation**

According to GDPdU, electronic evaluation must be provided. The data sourcing archiving system must have processing capacities, in a quantitative and qualitative degree, similar to that of the source system as if the data was still in the productive system (broadly paraphrased from the BMF pronouncement).

During a transfer no changes may occur to the object to be archived or to its ability to be evaluated.

With regard to generic digital documents, it is to be noted whether structural information is present in addition to content that is necessary for electronic evaluation.

For example, the “header“ of e-mails contains, amongst other information, details about the sender, recipient and coding and is considered part of the structural information.

In addition to the e-mail itself and the structural information, e-mail attachments are also of importance. They are to be taken into consideration when the tax relevance of an e-mail is evaluated and should maintain their capability to be evaluated during the entire archiving process.

## II. Completeness and unalterability

All data must be fully archived. Therefore data from the source system may not be filtered in any way.

Fiscal authorities attach great importance that no densification of information occur prior to acceptance by the archiving system or subsequently to acceptance, because a loss of tax-relevant information cannot be precluded.

The unalterability of archiving objects is to be ensured during all stages of the archiving process. The duplicability of the process is to be ensured through proper logging.

The applied archiving procedures have to be performed such that the following requirements are fulfilled:

- parameterisation of all systems of the archiving solution that ensure the capture of tax-relevant data
- loss-free data transfer to the data capture system
- prompt periodic archiving
- archiving of data true to the original in both imagery and content

## III. Secure and traceable data processing and data storage

Any subsequent changes to the archived objects must be prevented at all levels including the operating system, database and application level.

The complete storage of captured data is to be ensured in a retraceable manner and error-free saving is to be ensured by suitable plausibility controls.

To assure information security and data protection, the archiving software may allow for read-only data access in light of separation of functions and authorised interest, and as required in interaction with the operating system as well as applied third-party software (e. g. database system).

Thus, encrypted storage as well as encapsulation of the master file is permissible to the extent that the master file can be readably retrieved without causing a delay in the audit process.

Storage in a data format deviating from the master file is not acceptable and may act only as a supplement to the master file.

## IV. Adequate data accessibility

The applied archiving system must technically enable free access to data and documents.

To ensure prompt data access for fiscal authorities the archiving solution must allow for readability and reproducibility of the archiving objects at any time during the entire retention period.

In order to ensure the retrievability of tax-relevant e-mails, the requirements for proper filing must be satisfied. Therefore it is essential that each e-mail is assigned a unique index value.

Moreover the system should dispose of a suitable method for keyword indexing to map relations on data outside the archiving system. This ensures

that the tax auditor is able to retrace a logical chain of tax-relevant business transactions including the examination of particular data objects.

## **V. Assignment capability of e-mails and related business transactions**

The assignment of tax-relevant e-mails to corresponding business transactions is mandatory. This is rather complicated due to the characteristics of e-mails.

The following alternatives are possible:

- tax-relevant e-mails with reference to one business transaction
- tax-relevant e-mails with reference to numerous business transactions
- tax-relevant e-mails not in reference to any business transaction

Fiscal authorities do not provide specific operational guidelines on how such an assignment is to be made in a reliable manner. Insofar the taxpayer is not subject to any restrictions regarding his choice of procedures. A suitable archiving system should nevertheless provide for convenient methods to allow for such an assignment.

## **VI. Provision of adequate process documentation**

The archiving solution must dispose of an adequate process documentation, consisting of the following components:

- user documentation
- technical system documentation
- operational documentation

Therein the applicable procedures are to be determined and verified. This applies in particular to the controls designated to the respective procedures.

Moreover the process documentation shall contain technical (e. g. interface definitions to preceding and subsequent systems) and organisational definitions (e. g. point in time and frequency of archiving processes).

## **VII. Data protection requirements**

Along with the fundamental problem of automated e-mail qualification, using server-sided archiving in companies also includes difficulties with regard to data protection requirements.

Through server-sided automated archiving of e-mails, all incoming e-mails are captured before they reach the recipient's individual sphere of control on his workstation computer. In this case, private e-mails would also be subject to archiving.

## **D. Risks**

The risks resulting from a failure to satisfy statutory requirements are numerous. In addition to potential legal consequences, they primarily affect image, profitability and efficiency of the company.

Material risks are e. g.:

- non-deductibility of input VAT

- sanctions for non-compliance with regulations
- loss of evidentiary value
- data protection violations
- increased in-house expenses
- disclosure of sensitive internal information

### **Non-deductibility of input VAT**

As a result of inadequate or incomplete archiving of incoming invoices received by the company via e-mail in the context of transmission of electronic invoices (“e-billing”), there is a danger of losing the deductibility of input VAT.

In this context, the proper archiving of the so-called “validated electronic signature“, accompanying an electronic invoice must be considered. In Germany, the “Value Added Tax Act“ (Umsatzsteuergesetz, UStG) demands a validated electronic signature on electronically transmitted invoices in order for the company receiving the invoice to deduct the input VAT.

### **Sanctions for non-compliance with regulations**

Violations of regulations may result in sanctions by fiscal authorities ranging from penalties and fines on arrears for exceptionally severe violations that can amount to EUR 250,000 (§ 146 2b AO) and may extend to an estimation of the tax basis.

### **Loss of evidentiary value**

Inadequate archiving may result in a loss of evidentiary value and thus result in an indefinite financial risk.

This is particularly possible if the archived e-mails do not remain unaltered and in their original format, as required. For example, business correspondence between customers and suppliers may represent essential evidence in litigation where the content and sequence of events are material.

### **Data protection violations**

Violations of data protection requirements are especially possible as a result of insufficient physical and logical access restrictions to material data if access to or even manipulations of personal data are thereby possible.

A violation of data protection regulations may result in substantial monetary fines ranging, in the worst case, from EUR 50,000 as a consequence of violations of procedural rules to EUR 300,000 for violations of material data protection regulations.

### **Increased in-house expenses**

The in-house expense of providing prompt and free data access to fiscal authorities must also be considered.

For example, a subsequent sorting of a progressive increase of e-mail data may result in a considerable operating expense.

In contrast, proper filing normally results in

significant efficiency advantages.

In addition, the implementation of a dedicated e-mail archiving solution avoids unnecessary data redundancy and excess use of resources (e. g. storage capacity).

### **Disclosure of sensitive internal information**

The fiscal authorities are not subject to any restrictions regarding exploitation of information that has accidentally come into their possession or which exceeds the object of the audit.

Failed or flawed separation of tax-relevant e-mails from non tax-relevant e-mails may lead to a situation where, as a result of the disclosure of internal information which was not an object of the audit, fiscal authorities could acquire facts that might be to the company's disadvantage. This represents an avoidable risk.

## E. GFI MailArchiver 6 Checklist

### System Design

#### Selection of a suitable archive storage

- Does the selected archive storage comply with the requirements of unalterable and traceable archiving?

It is essential that the archive storage allows for comprehensive logging of all saving processes and subsequent data access (including the database level).

The database system MS SQL Server serves as a suitable data storage.

Subject to appropriately configured access rights the above referenced requirements are fulfilled by complete storage of all data within the database to enable GDPdU-compliant storage.

#### Security of data connection

- Does the archiving of e-mails occur via network connections from source systems that are not located within the user's sphere of confidence (e. g. from remote MS Exchange Servers)?

In this case unalterability within the transmission path has to be ensured by encryption protected file transfer.

For this purpose it is necessary to select the transmission protocol IMAP with secure sockets layer (SSL) in GFI MailArchiver to connect with the source system.

### Parameterisation and interfaces

In order to allow for a configuration of the archiving solution that complies with the requirements of GDPdU, the following mandatory preparations on the side of the source system (MS Exchange Server) are to be made prior to the initial operation:

- Definition and installation of the journaling mailbox that is to contain all e-mails designated for archiving of the corresponding server
- Activation of envelope journaling in MS Exchange Server to ensure the completeness of the scope of archiving, comprising all possible e-mail recipients including blind carbon copy recipients (BCC)  
This feature is already activated by default when using MS Exchange Server 2007.
- Activation of the message tracking function to allow for subsequent verification of complete archiving

In addition to the mandatory preparations for GDPdU-compliant archiving, the following recommendations should be considered:

- Is it ensured that the scope of e-mails designated for archival storage is not limited by archiving option settings of GFI MailArchiver?

With regard to completeness aspects the following settings are to be made:

- Capture of e-mails in all possible directions (incoming, outgoing and internal)
- No exclusions based on blacklisted user

accounts of the windows domain or specific e-mail addresses

- No limitations on the number of users based on whitelisted user accounts of the windows domain or specific e-mail addresses

Exceptions result from user accounts or e-mail addresses where tax relevance of the e-mail traffic can definitely be excluded.

- ❑ Is it ensured that no archiving policies are installed which allow for a storage time shorter than the statutory retention period (e. g. retention policies for immediate deletion based on predefined features)?

### Processes and organisation

- ❑ Does the written definition serve as a suitable method to allow a competent third party to comprehend content, structure and process flow of the procedures within an appropriate timeframe?
- ❑ Are all responsibilities for the particular process steps (functional and IT related operations) for all archiving components fully defined?
- ❑ Is it ensured that users are instructed on how to operate the archiving system and/or is a user manual placed at their disposal?
- ❑ Is it ensured that the system administration is instructed on how to operate the

archiving system and/or is an administration manual placed at its disposal?

- ❑ Are maintenance and operations control tasks of the archiving system properly defined and contained in a superordinated concept of IT related controlled operations?
- ❑ Are all verification tasks properly defined?
- ❑ Does the configured authorisation concept comply with the predetermined competencies and is the procedure adequately documented?

### Capture

- ❑ Are all procedures and techniques that allow for verifiable complete and correct capture and archival storage of e-mails properly defined and documented?

GFI MailArchiver does not support the logging of e-mails transferred via standard interface from MS Exchange Server. Therefore the verification of loss-free and thus complete data transfer, according to the requirements of GDPdU, must be provided by the logging protocol generated by the particular source system (MS Exchange Server).

If necessary, it is possible to verify complete archiving by comparison of the logging protocols (which are generated by the message tracking function of MS Exchange Server and show the processed e-mails) with the subsequently stored e-mails in the archive on the basis of common identifying features.

- ❑ Are suitable procedures in place that ensure compliance with the requirements of GDPdU with regard to the archival storage of signed and encrypted e-mails?

A subsequent editing of archived e-mails and the combined capture of e-mails with additional data sets that are not directly obtained from MS Exchange Server are not supported by GFI MailArchiver. Therefore appropriate procedures should be installed (e. g. manual keyword indexing) to allow for an assignment of signed or encrypted e-mails to their corresponding verification records or decrypted e-mails and related decryption keys.

## Indexing and keyword indexing

- ❑ Are the procedures for the labelling of tax-relevant archived e-mails unambiguously specified?

There are two fundamentally different options provided by GFI MailArchiver 6 on how labels can be attached to e-mails:

- Automatically through policy-based labelling at the moment of archiving by means of definable categorisation policies
- Manually through subsequent manual labelling of archived e-mails that are accessible to the user

It is advisable to refrain from a policy-

based automated labelling – especially as a sole technique. An evaluation of tax relevance is usually too complex for predetermined policies to operate in a reliable manner.

In any case, such policy-based automated procedures should be accompanied by a manual verification.

- ❑ Has a procedure been defined that allows for an assignment to one or multiple business transactions by means of a suitable keyword indexing in GFI MailArchiver?

The option provided by GFI MailArchiver to individually apply labels visible to all users to e-mails that are accessible by the user allows, in addition to a labelling of tax relevance, for a direct assignment to a corresponding business transaction.

This can be implemented by applying a label (e. g. keyword index) that contains identifying features allowing for a retrieval of corresponding content in other systems.

- ❑ Has a procedure been defined that allows for a distinct assignment of the archived e-mails in a separate accounting system?

In this regard, the identifier (“Identification Code“) that enables distinct identification of archived e-mails within GFI MailArchiver is important.

Assimilated in an external system (e. g. ERP system ), this identifier can serve as a so-called “foreign key” to establish a logical reference to

the related e-mails and, in this way, an assignment to the business transaction.

The "Identification Code" accessible at the application level provides valuable help in enabling technical usage of such a foreign key reference in a networked system environment.

Subject to appropriately set up access rights, the archived e-mails can be directly addressed out of external systems via hyperlink. However, for this to function, it is necessary that the referencing system contain a method to generate the uniform resource locator (URL) autonomously. The utilisation of GFI MailArchiver's identifier "Identification Code" to serve as a referencing linkage out of an external software system is possible using the therein contained parameters "id" and "connectionId".

Such a URL can be composed as follows:

- Addressing the user interface of GFI MailArchiver to view the e-mail:  
<http://localhost/mailarchiver/mailview.aspx?>
- Addition of the ("id") representing the active archive store of GFI MailArchiver:  
<http://localhost/mailarchiver/mailview.aspx?id=-2147483647>

- Addition of the second parameter, the Connection-ID ("connectionId"):  
<http://localhost/mailarchiver/mailview.aspx?id=-2147483647&connectionId=b44d3270-8bdb-43d2-8fa2-67eb6ead54a9>

Entering the URL results in a view of the specific e-mail in the archive:

<http://localhost/mailarchiver/mailview.aspx?id=-2147483647&connectionId=b44d3270-8bdb-43d2-8fa2-67eb6ead54a9>

### Storage and administration

- Is it ensured that the selected archive storage provides the foreseeably required storage capacity and that this is monitored regularly?
- Is it ensured that subsequent verifiability of complete archiving based on a comparison of e-mails transferred by MS Exchange and e-mails archived by GFI MailArchiver (preferably by means of their message-id) is possible?

Accordingly, it is necessary to assure that the MS Exchange Server logs which enable the comparison on the source side be stored loss-free (e. g. no overwriting, only append mode) as long as the archived data itself.

### Readability and retrieval

- Is a tax auditor user account set up that enables access to all tax-relevant e-mails?

As GFI MailArchiver does not support or allow for restricted access based on labels, it is advisable to install an organisational procedure for labelling tax relevance to ensure separation of data within the archive prior to a tax audit (e. g. systematic designation of tax relevance using the manual method for individual labelling).

In a further step, an export based on such labels followed by a subsequent reimport into a dedicated archive store can be conducted in preparation of a tax audit. In this way a tax auditor is granted comprehensive access to exclusively tax-relevant e-mails based on labels.

## Retention and deletion

- Is it ensured that no retention policies are defined that cause a deletion of archived e-mails prior to expiration of the statutory retention period?

Some tax-relevant e-mails – in certain cases – may contain information that requires a retention period of ten years.

Therefore it is advisable to refrain from a policy-based determination of the retention period by means of the retention policies of GFI MailArchiver to the extent that they do not correspond with the longest statutory minimum period for retention.

## Software security

- Is there an authorisation concept that allows for a determination of the required separation of functions and the assignment of access rights?
- Are adequate access controls available at the following access levels:
  - operating system  
MS Windows including Active Directory, web server and MS Exchange Server
  - database system  
MS SQL Server
  - archiving software  
GFI MailArchiver 6

## Process documentation

- Are all settings regarding the parameterisation of software and interfaces properly documented?
- Are all interfaces between the particular components of the archiving solution (e. g. designation, source/destination system, interface content/type, matching) documented in a comprehensible manner?
- Are the interfaces between the archiving solution and other software systems of the company (e. g. ERP system or financial accounting system) with regard to referencing business transactions documented in a comprehensible manner?
- Are operating instructions for users available that allow for proper performance of their

activities including the manual controls and matching (operational documentation) provided by the procedure?

- ❑ Is a description of the applied components available that illustrates the technical architecture of the archiving solution and how the operational requirements are realised (technical system documentation)?
- ❑ Are operating instructions for IT personnel available that allow for proper performance of controlled operation (e. g. backup and restoration manual)?
- ❑ Is it ensured that the documentation of all effective procedures is archived as a document subject to retention?

### **Implementation and change**

- ❑ Is ensured that the compliance and security of the applied systems and software are subject to functional and technical test procedures prior to the initial operation of the archiving solution?
- ❑ Is a test procedure defined and documented and do the test cases allow for a verification of the requirements regarding compliance and security?
- ❑ Is a release procedure defined and documented that contains rules on release competencies and are release approvals for all components of the archiving solution available?

- ❑ Is it ensured that changes to the e-mail archiving solution are only applied subject to an orderly procedure (change management)?

### **IT operations**

- ❑ Are the IT operations (controlled and emergency operations) properly defined in organisational instructions (e. g. tasks and authority of administrators, rules for change management and the administration of storage media)?
- ❑ Has an emergency concept been prepared for a possible failure of the archiving solution (e. g. disaster recovery and contingency plan)?
- ❑ Are suitable data backup and data backup safekeeping procedures defined and are regular verification tests scheduled concerning effective data recovery?

### **Outsourcing**

- ❑ When engaging an external service provider to operate the archiving solution (outsourcing), is it ensured that the requirements regarding compliance and security are guaranteed by the service provider?

Appropriate contractual provisions and service level agreements are required.