Whitepaper und Prüfungsbericht:

Prüfbericht des GFI Archiver

PRWRECHTSANWÄLTE

GFI Archiver™

Optimierte Produktivität, Verwaltung und Compliance dank E-Mail-Archivierung

Inhaltsverzeichnis

A. Einleitung

A.
Einleitung

I. Prüfungsgegenstand und Prüfungszeitraum

(1) Gegenstand des Berichts ist die rechtliche Prüfung des „GFI Archiver 2015" im Hinblick auf dessen Vereinbarkeit mit den Anforderungen des Bundesdatenschutzgesetzes (BDSG), den Anforderungen bezüglich der Bestimmungen des Betriebsverfassungsgesetz (BetrVG) sowie den rechtlichen Bestimmungen über die Archivierungspflicht von geschäftlichen Unterlagen (GoBD).

(2) Die Prüfung erfolgte im Zeitraum zwischen dem 01.12.2014 und dem 15.12.2014.

(3) Im Rahmen der Prüfung wurde eine Vollversion des „GFI Archiver 2015" auf dem lokalen Netzwerk installiert. Der besseren Darstellung und der übersichtlicheren Dokumentation wegen, wurde bei der Auswertung auf die offiziellen Screenshots zurückgegriffen.

II. Hintergründe zum GFI Archiver 2015

(1) Der „GFI Archiver 2015" ist eine Archivierungslösung, mit deren Hilfe die internen und externen E-Mails des Unternehmens zentral gespeichert und verwaltet werden können. Darüber hinaus können die Benutzer archivierte E-Mails, einschließlich der Anlagen und Inhalte, durchsuchen und einzeln abrufen. Daneben besteht die Möglichkeit, sonstige Dateien und Kalenderdaten zu speichern, einheitlich zu sichern und bei Bedarf von den Benutzern zentral zu verwalten.

(2) Ein wesentlicher Bestandteil des „GFI Archiver 2015" ist das Reporting-Tool MailInsights, mit dessen Hilfe die E-Mail-Archive auf wichtige geschäftsrelevante Unterlagen und Informationen hin untersucht werden können. Gleichzeitig gewährleistet MailInsights den zentral gesteuerten Schutz vor potenziellen Sicherheitsrisiken und den damit drohenden rechtlichen Gefahren oder Produktivitätsproblemen[1].

B. Auswertung des GFI Archiver 2015

B.
Auswertung des GFI Archiver 2015

I. Grundlagen der Archivierung

1. Archivierungspflicht

(1) Ein spezielles Gesetz zur Archivierung, bzw. zur E-Mail-Archivierung gibt es nicht. Es existieren jedoch zahlreiche rechtliche Vorschriften aus unterschiedlichen Rechtsgebieten, die eine Aufbewahrungspflicht (Archivierung) normieren. Die zentralen Vorschriften in Bezug auf die Aufbewahrungspflicht von E-Mails für den „GFI Archiver 2015" stammen aus dem Handels- und Steuerrecht. Gemäß §§ 238, 257 HGB besteht für einen Kaufmann die Verpflichtung, eine Kopie der abgesendeten Handelsbriefe zurückzubehalten bzw. sicher auf-zubewahren.

1 Weitere technische Einzelheiten finden Sie unter:
http://www.gfisoftware.de/products-and-solutions/email-and-messaging-solutions/gfi-mailarchiver

- Vollständigkeit (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB)
- Richtigkeit (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB)
- Zeitgerechtheit (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB)
- Unveränderbarkeit (§ 146 Abs. 4 AO, § 239 Abs. 3 HGB)
- Ordnung (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB) und der
- Nachvollziehbarkeit (§ 145 Abs. 1 AO, § 238 Abs. 1 Satz 2 HGB).

5. Sanktionen

(1) Der Verstoß gegen eine ordnungsgemäße Archivierung kann erhebliche Rechtsfolgen nach sich ziehen. So kann die unterlassene Archivierung als Verletzung der handelsrechtlichen oder steuerrechtlichen Buchführungspflicht gewertet oder als Ordnungswidrigkeit geahndet werden (§ 379 AO). Zudem ist auch eine straf-rechtliche Bewertung gemäß § 283b StGB nicht ausgeschlossen.

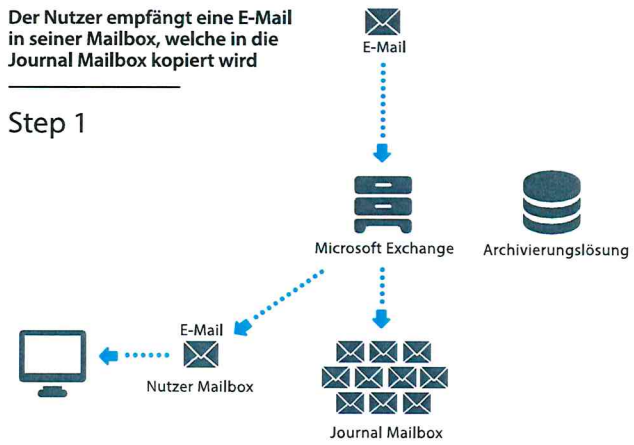
(2) Geschäftsführer oder Vorstände der betroffenen Gesellschaften haften nach § 43 Abs. 2 GmbHG, § 93 Abs. 2 AktG.

II. Bewertung des GFI Archiver 2015 anhand GoBD

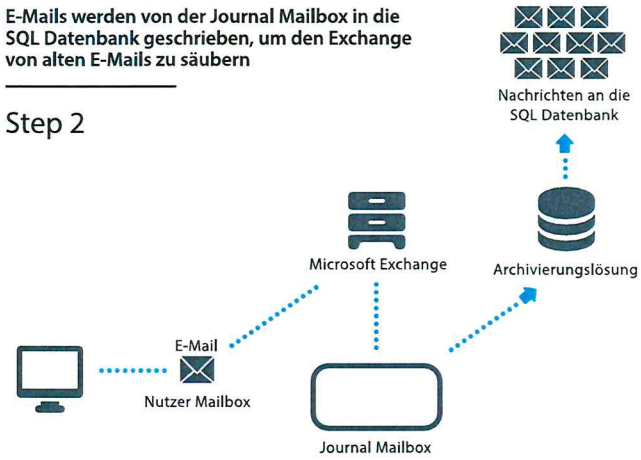
1. Vollständigkeit

(1) „Vollständigkeit" (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB) bedeutet die lückenlose Erfassung aller buchungspflichtiger Geschäftsvorfälle, Daten und Unterlagen.

(2) Der „GFI Archiver 2015" setzt diese Vorgabe mittels der Funktion des sog. „Journaling" um. Hierbei werden sämtliche eingehenden und ausgehenden E-Mails des Unternehmens zunächst auf einem MS-Exchange Server kopiert. Sollen nur bestimmte Nachrichten automatisch gesichert werden, können entsprechende Auswahlkriterien anhand von flexiblen Archivierungsregeln festgelegt werden.



- Abbildung: 1 -



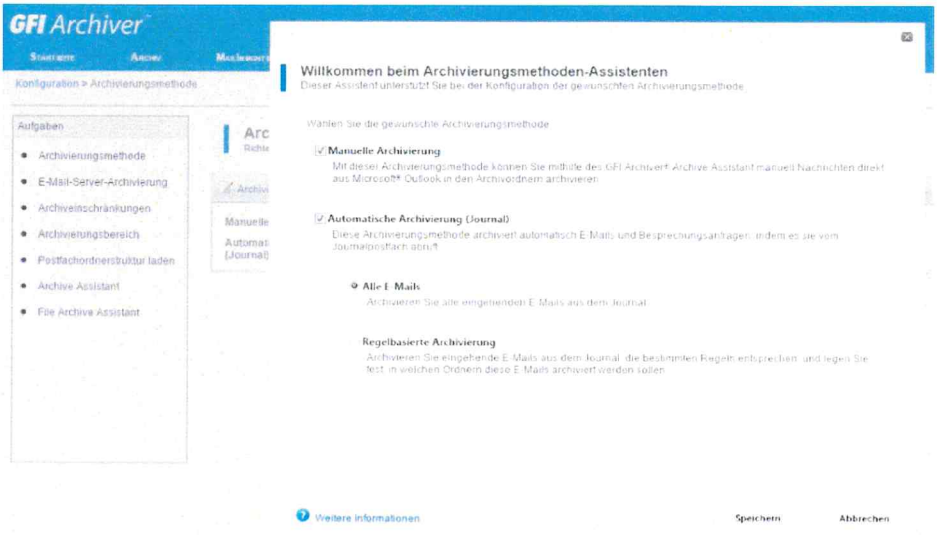
- Abbildung: 2 -

(3) Aufgrund dieses automatisierten Kopiervorgangs können die eingehenden oder ausgehenden E-Mails von den Benutzern weder verändert noch gelöscht werden. Eine manuelle Löschung einer E-Mail, bzw. der „pst-Datei", bleibt im Journal in der ursprünglichen Fassung bestehen. Im Zweifel ist damit im Nachhinein stets nachprüfbar, ob eine Änderung, Verfälschung oder Löschung der Daten stattgefunden hat.

(4) Die Vorgabe des Kriteriums der „Vollständigkeit" ist damit erfüllt.

2. Richtigkeit

(1) Das Erfordernis der „Richtigkeit der Daten und Unterlagen" bedeutet, die Geschäftsvorfälle in Übereinstimmung mit den tatsächlichen Verhältnissen und im Einklang mit den rechtlichen Vorschriften inhaltlich zu-treffend durch entsprechende Belege abzubilden.

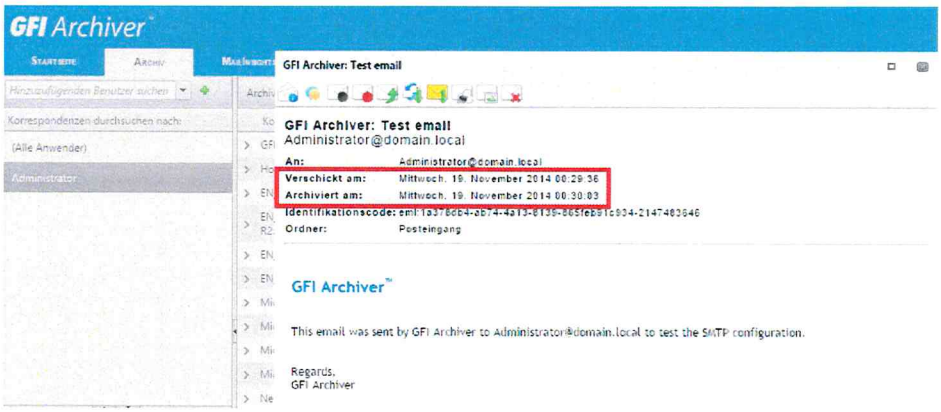


- Abbildung: 3 -

(2) Die Vorgaben können mit Hilfe des „GFI Archiver 2015" rechtskonform umgesetzt werden.

3. Zeitgerechtheit

(1) Die Zeitgerechtheit umfasst sowohl die Zuordnung der Geschäftsvorfälle zu bestimmten Buchungszeitpunkten (Periodengerechtigkeit), als auch die zeitliche Nähe zum Eingang der zu archivierenden Nachrichten.



- Abbildung: 4 -

(2) Mit Hilfe der umfassenden Einstellungsmöglichkeiten kann eine zeitgerechte Archivierung und Erfassung der Geschäftsunterlagen und Buchungsbelege gewährleistet werden.

4. Unveränderbarkeit

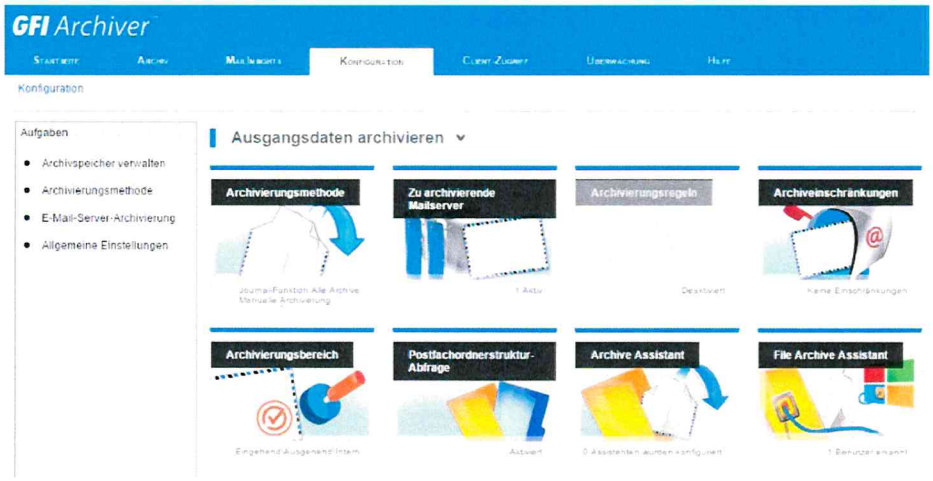
(1) Nach dem Grundsatz der Unveränderbarkeit (§ 146 Abs. 4 AO und § 239 Abs. 3 HGB) dürfen Änderung von Eintragungen oder Aufzeichnungen nur auf die Art erfolgen, dass der ursprüngliche Inhalt und die Tatsache, dass eine Änderung stattgefunden hat, sowie die zeitliche Abfolge und Wirkung der Änderung erkennbar bleiben und entsprechend protokolliert werden („Kopie").

- Abbildung: 5 -

(2) Wie bereits oben („Vollständigkeit" der Datenerfassung) dargestellt, kann nach Eingang oder nach dem Versand einer Nachricht mittels der „Journaling-Funktion" eine Kopie in dem Journal erstellt werden. Ab diesem Zeitpunkt ist eine Änderung oder Löschung nicht mehr möglich. Das Kriterium der „Unveränderbarkeit" der Daten wird erfüllt.

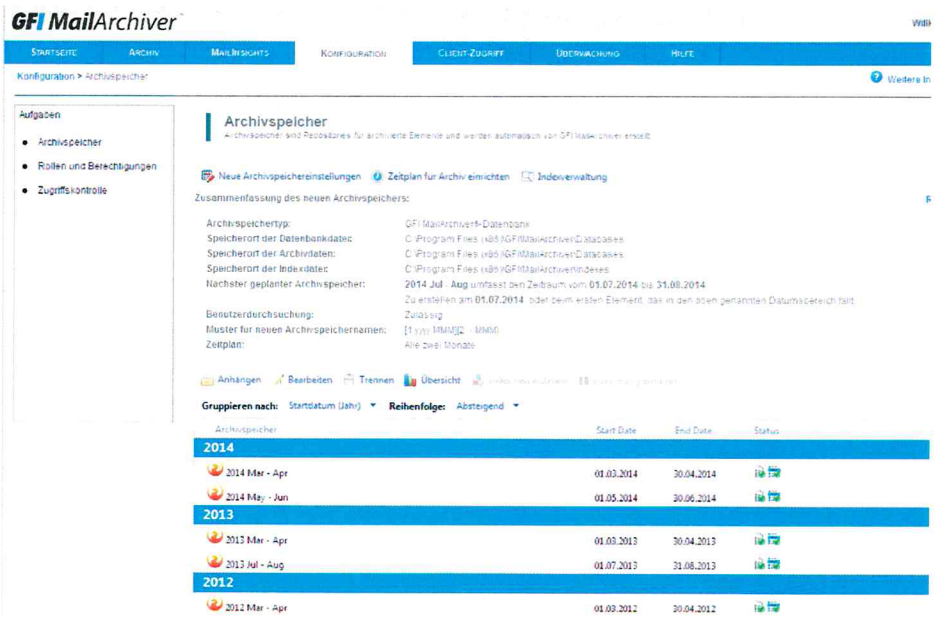
5. Nachvollziehbarkeit und Nachprüfung

(1) Der Grundsatz der Nachvollziehbarkeit und Nachprüfung besagt, dass ein sachverständiger Dritter innerhalb angemessener Zeit in der Lage sein muss, sich auf Grundlage des eingerichteten Buchführungssystems einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens zu verschaffen. Hierzu gehören systematische Verzeichnisstrukturen, insbesondere eine zeitlich geordnete Ablage, sodass ein geordneter Zugriff des Prüfers auch ohne Fremdhilfe möglich ist. Die Entstehung und die Abwicklung jedes einzelnen Geschäftsvorfalls sowie das dabei angewendete Verfahren müssen intersubjektiv nachvollziehbar sein (§ 238 Abs. 1 S. 3 HGB).



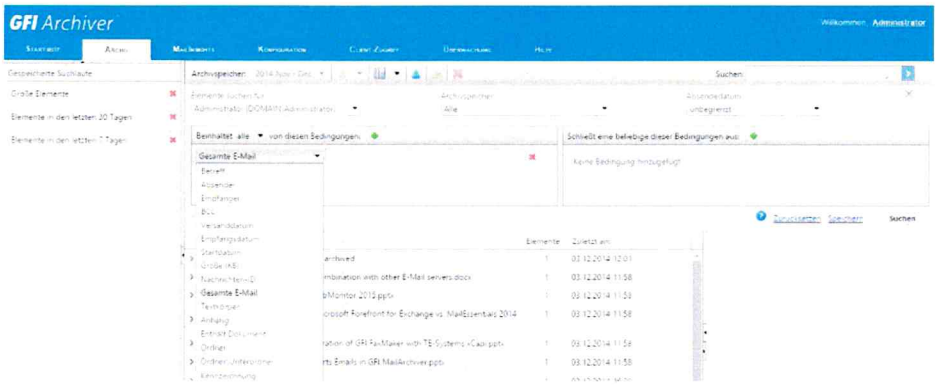
- Abbildung: 6 -

(2) Der „GFI Archiver 2015" stellt diverse Funktionalitäten zur Verfügung, um gespeicherte Nachrichten, Daten und Informationen zu recherchieren und abzurufen. So erhält der Administrator die Möglichkeit, die archivier-ten Nachrichten gesondert zu verwalten und je nach Jahrgang in unterschiedlichen Verzeichnissen (Datenbanken) anzeigen zu lassen.



- Abbildung: 7 -

(3) Desweiteren können die Nachrichten anhand von Begriffen durchsucht werden, wodurch ein schneller Zugriff auf die relevanten Informationen ermöglicht wird.



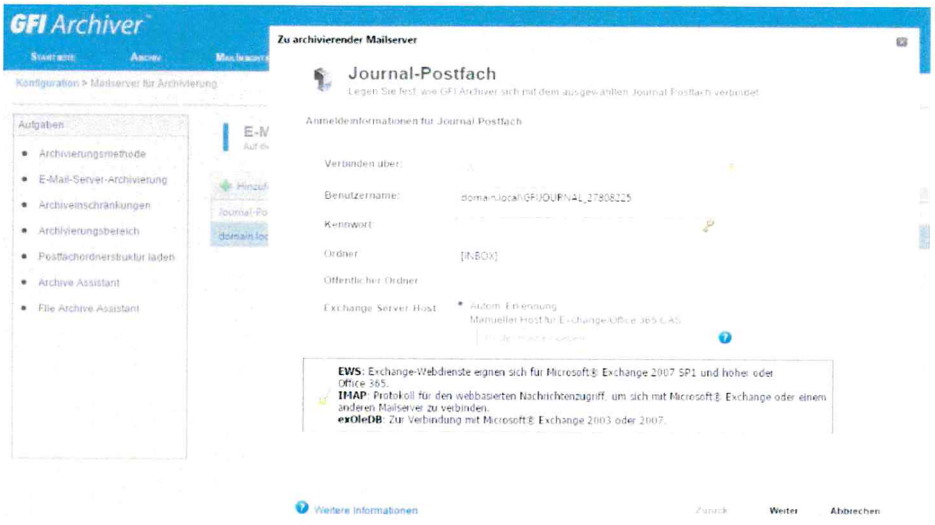
- Abbildung: 8 -

(4) Der Administrator und Nutzer des „GFI Archiver 2015" hat dabei die Möglichkeit, bestimmte Schlagworte zu vergeben, um Verzeichnisstrukturen zu erstellen oder eine spätere Auffindbarkeit von gesuchten E-Mails zu erleichtern und für Dritte bei Bedarf sicher zu stellen.

6. Übereinstimmung

(1) Bei der Wiedergabe von geschäfts- und steuerrelevanten Unterlagen über einen E-Mail-Client ist die bildliche Übereinstimmung der Geschäftsbriefe und Buchungsbelege zu gewährleisten. Das bedeutet, dass die Informationen des Ausgangsdokuments in die elektronische Form übernommen werden, in dem u. a geregelt wird, zu welchem Zeitpunkt das Dokument erstellt wurde und ob eine bildliche oder inhaltliche Übereinstimmung mit dem Original erforderlich ist. Im Ergebnis muss sichergestellt sein, dass das Zieldokument mit dem Ausgangsdokument übereinstimmt.

(2) Der „GFI Archiver 2015" gewährleistet mittels der Journaling-Funktion, dass alle versandten und empfangenen, internen und externen E-Mails mit sämtlichen Anhängen im Archiv identisch verfügbar sind und mit dem Ursprungsdokument übereinstimmen.



- Abbildung: 9 -

III. GoBD-Compliance

1. Betriebsprüfung

(1) Die Finanzverwaltung hat nach § 147 Abs. 6 AO das Recht (§ 5 AO), im Rahmen einer Außenprüfung Einsicht in die gespeicherten Daten der Steuerpflichtigen zu nehmen.

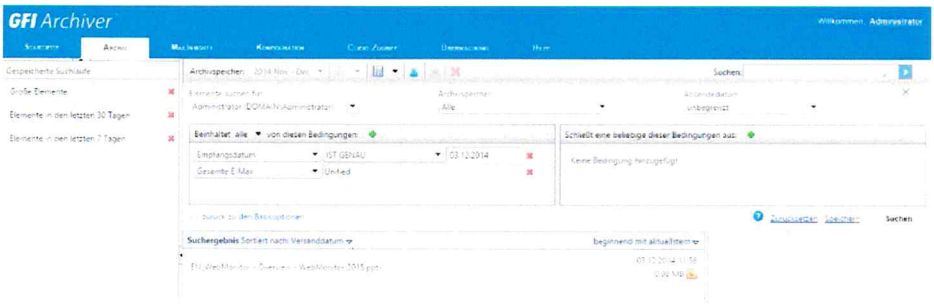
(2) Der Betriebsprüfer hat dabei die Möglichkeit, unmittelbar Einsicht in die vom Steuerpflichtigen gespeicherten Daten zu nehmen und zur Prüfung der gespeicherten Daten das Datenverarbeitungssystem des Steuerpflichtigen zu nutzen (sog. unmittelbarer Datenzugriff).

(3) Darüber hinaus kann der Prüfer den Steuerpflichtigen nach § 147 Abs. 6 S. 2 Alt. 1 AO auffordern, Daten nach seinen Vorgaben vor Ort in seinem Datenverarbeitungssystem auszuwerten (sog. mittelbarer Datenzu-griff). Zuletzt kann der Prüfer nach § 147 Abs. 6 S. 2 Alt. 2 AO verlangen, dass der Steuerpflichtige ihm seine gespeicherten Unterlagen auf einem maschinell verwertbaren Datenträger zur Verfügung stellt (sog. Datenträgerüberlassung).

(4) Mit Hilfe des „GFI Archiver 2015" können diese Vorgaben umgesetzt werden.

2. Unmittelbarer Zugriff

(1) Die Einsichtnahme in gespeicherte Daten und die Nutzung des Datenverarbeitungssystems des Steuerpflichtigen wird dadurch gewährleistet, dass der Betriebsprüfer Zugriffsmöglichkeiten und umfassende Recherchetools (Suchfunktion) nutzen kann, um E-Mails und E-Mail-Anhänge zu suchen.



- Abbildung: 10 -

(2) Die Anforderungen des § 147 Abs. 6 AO werden erfüllt.

3. Mittelbarer Zugriff

(1) Dem Verantwortlichen steht nach denselben Kriterien die Möglichkeit offen, technische Mithilfe zu leisten, um dem Betriebsprüfer die gewünschten Informationen zukommen zu lassen, bzw. nach dessen Vorgaben die E-Mails zu durchsuchen.

(2) Die Anforderungen des § 147 Abs. 6 AO werden auch insoweit erfüllt.

4. Datenträgerüberlassung

(1) Zur Ausübung des Datenzugriffs kann die Außenprüfung als dritte Möglichkeit verlangen, dass die gespeicherten Unterlagen und Aufzeichnungen, bzw. E-Mails, auf einem maschinell verwertbaren Datenträger (z. B. DVD) zur Verfügung gestellt werden.

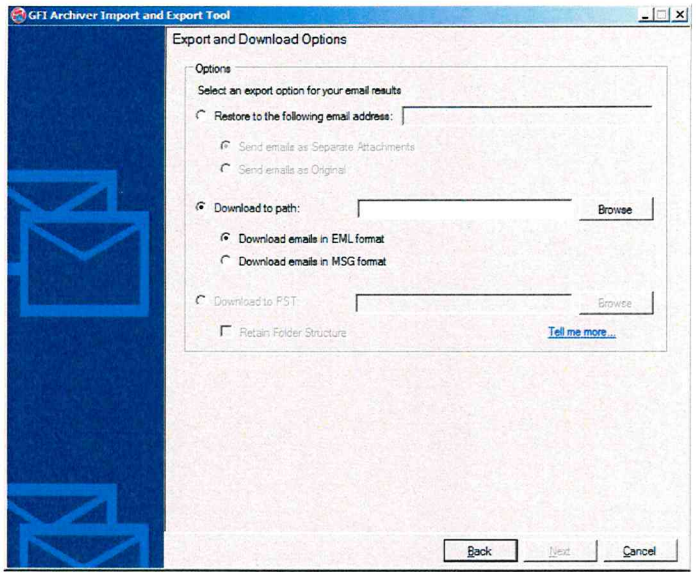
(2) Mit Hilfe des „GFI Archiver 2015" können die steuerlich relevanten Daten und Dokumente exportiert werden, um diese auf einem externen Trägermedium den Steuerbehörden zur Verfügung zu stellen.

- Abbildung: 11 -

(3) Die vorgelagerte Herausforderung des Unternehmens, steuerlich nicht relevante oder dem Berufsgeheimnis (§ 102 AO) unterliegende Daten Zugriffsbeschränkungen zu unterwerfen, um damit sicherzustellen, dass die Außenprüfung auf diese Daten nicht zugreifen kann, werden durch die Möglichkeit der Indexierung und Sortierung gewährleistet. Insoweit bedarf es einer klaren Dateistruktur, die zwischen steuerlich relevanten Daten einerseits und steuerlich nicht relevanten personenbezogenen oder dem Berufsgeheimnis (§ 102 AO) unterliegenden Daten andererseits differenziert. Diese Trennung ist mit dem „GFI Archiver 2015" möglich. Gleichzeitig besteht die Möglichkeit, eine Protokollierung vorzunehmen, um nachvollziehen zu können, auf welche Daten die Außenprüfung tatsächlich zugegriffen hat.

5. Systemwechsel und Migration

(1) Im Zusammenhang mit dem Datenzugriff der Finanzverwaltung stellen sich bei Archivlösungen weitere Herausforderungen im Hinblick auf die Kontinuität der Zugriffsmöglichkeiten, die sich in Folge von Änderungen der Soft- und Hardwareumgebung ergeben.



- Abbildung: 12 -

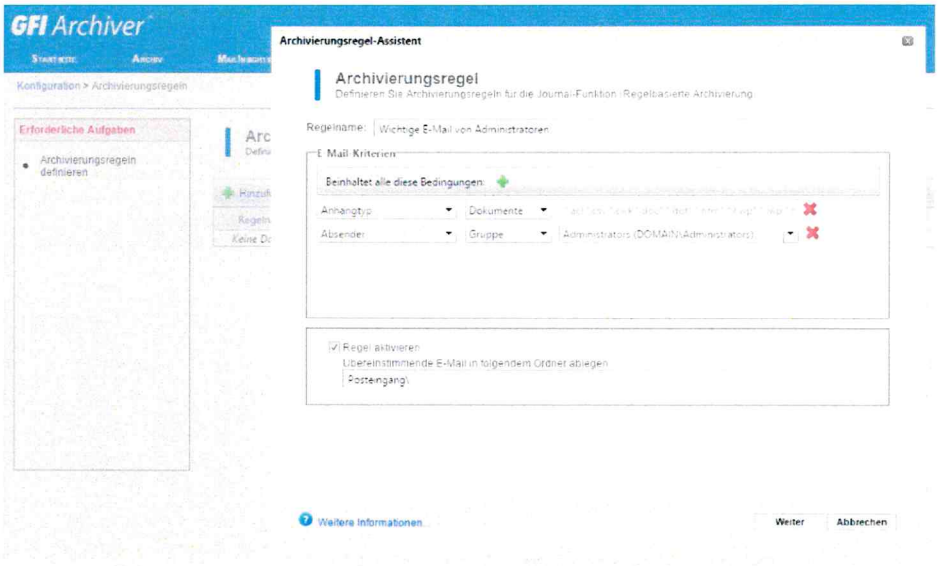
(2) Um diese Zugriffsrechte zu gewährleisten, wird in den §§ 146 Abs. 5 S. 2, 3 AO i. V. m. § 147 Abs. 6 AO angeordnet, dass bei der Führung der Bücher und der sonst erforderlichen Aufzeichnungen auf Datenträgern sichergestellt sein muss, dass während der Dauer der Aufbewahrungsfrist die Daten jederzeit verfügbar sind und unverzüglich lesbar gemacht werden können. Daraus ergibt sich auch das Erfordernis der maschinellen Auswertung. Im Hinblick darauf ergibt sich die Notwendigkeit, das EDV-System für die gesamte Dauer der Aufbewahrungsfrist für Zwecke des Datenzugriffs vorzuhalten oder aber bei einem Wechsel des EDV-Systems sicherzustellen, dass der Datenzugriff bei einer Außenprüfung unverändert möglich bleibt.

(3) Die von einem Unternehmen eingesetzte E-Mail-Archivierungslösung muss daher die Problematik des Systemwechsels und der Migration von Daten beherrschen. Die Archivierungslösung „GFI Archiver 2015" ermöglicht eine verlustfreie Überleitung der Alt-Datenbestände zum neuen Archiv. Umfangreiche Import- und Exportfunktionalitäten gewährleisten, dass Daten in das System importiert und aus dem System exportiert werden können, um die notwendige Kontinuität der Datenhaltung im Archiv sicher zu stellen.

6. Trennung von sensiblen Daten

(1) Der „GFI Archiver 2015" ermöglicht regelbasierte Ausnahmen, die z.B. die Kommunikation mit dem Betriebsrat von der Archivierung ausnehmen. Hierdurch können über die Einrichtung separater E-Mail-Adressen bestimmte sensitive E-Mails (z.B. des Betriebsrates oder Betriebsarztes) vom Journaling und damit von der Archivierung ausgenommen werden.

(2) Eine vertrauliche Kommunikation ohne Archivierung ist damit möglich.



- Abbildung: 13 -

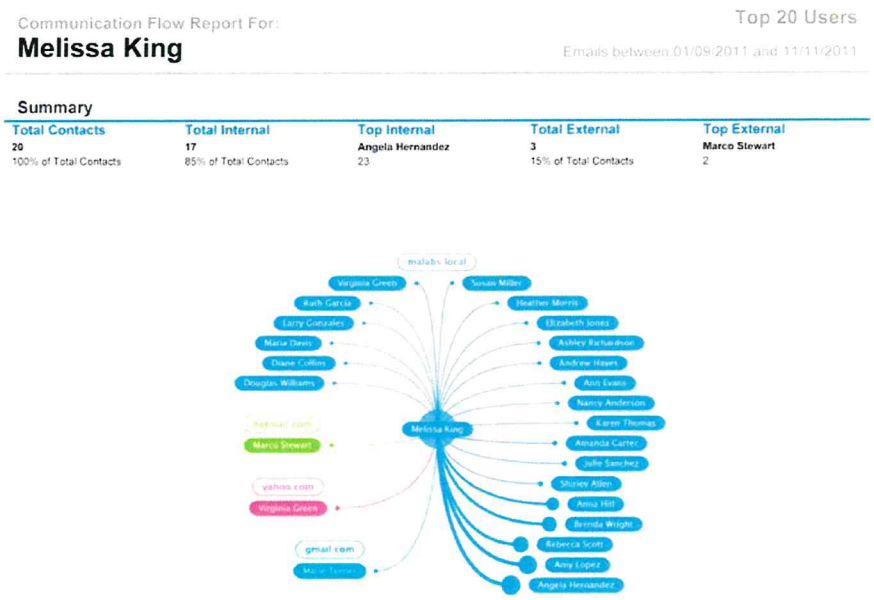
7. Data Loss Prevention und Monitoring

(1) Der Umgang und die Sicherung von unternehmensrelevanten und personenbezogenen Daten stellen ein wesentliches rechtliches, wie auch wirtschaftliches Gut eines Unternehmens dar. Nicht zuletzt aufgrund der Vielzahl von Schnittstellen und externen Kommunikationsvorgängen trifft diese Herausforderung auf die Gefahr, diese Daten durch Diebstahl, Hackerangriffe oder auch nur aufgrund fahrlässigen Verhaltens der Mitar-beiter zu verlieren. Zur Erfüllung der betrieblichen Organisationspflichten, wie auch der Vorgaben aus dem Risiko- und Informationssicherheitsmanagement ist die Geschäftsleitung zur Abwehr der drohenden Gefahren verpflichtet.

(2) Hier setzen sog. „Data Loss Prevention"-Konzepte (DLP) an, die es ermöglichen sollen, die Nutzung von IT-Systemen und Endgeräten zu überwachen. Hierzu zählt z. B. die Möglichkeit, Daten auf der Grundlage bestimmter Regelwerke zu erkennen, zu klassifizieren und weiteren Schutzmechanismen (z.B. einer Verschlüs-selung) zuzuweisen. Mithilfe der DLP-Technik lassen sich z.B. auch Zugriffs- und Versendeberechtigungen überwachen, Datenverarbeitungsvorgänge protokollieren und kontrollieren, Nutzer auf bestimmte Ge- oder Verbote während der Datenverarbeitung hinweisen, zentrale Stellen bei Regelverstößen alarmieren und der Zugriff auf bestimmte Daten verhindern.

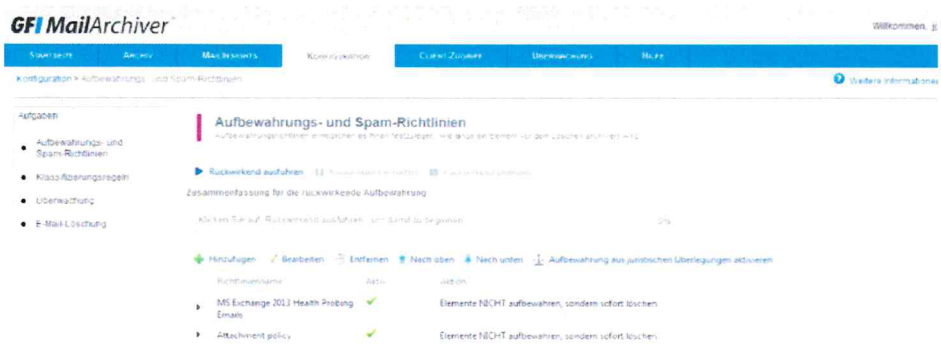
(3) Damit können DPL-Systeme wichtige, je nach Einzelfall eventuell sogar zentrale Bausteine eines IT-Sicherheitssystems sein.

(4) Der „GFI Archiver 2015" setzt diese Anforderung um, indem bestimmte Inhalte und deren autorisierte Nut-zung anhand vordefinierter Regelwerke (Policies) definiert und überwacht werden können. Auch Zugriffs- und Versendungsrechte können hierbei verwaltet und dokumentiert werden.



- Abbildung: 14 -

(5) Der Schutz vor ungewolltem „Datenverlust" wird auch durch das Feature unterstützt, das den Zugriff auf bestimmte E-Mails und Dokumente verhindert. Die notwendige Güterabwägung zwischen den Interessen der betroffenen Mitarbeiter (Beteiligungsrechte des Betriebsrats sind zu beachten) und des Unternehmens, können auf Basis einer Datenklassifizierung erfolgen, bei der der Umgang mit besonders werthaltigen oder sensiblen Firmendaten besonders protokolliert wird.



- Abbildung: 15 -

(6) Mittels des „GFI Archiver 2015" sind die rechtlichen Vorgaben an die Grundsätze der GoBD erfüllt, bzw. können vom Nutzer rechtskonform umgesetzt und berücksichtigt werden.

(7) Insgesamt werden die nachfolgenden Kriterien zusammenfassend erfüllt:

Anforderung	
1. Jedes Dokument muss nach Maßgabe der rechtlichen und organisationsinternen Anforderungen ordnungsgemäß aufbewahrt werden können.	✓
2. Die Archivierung hat vollständig zu erfolgen – kein Dokument darf auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.	✓
3. Jedes Dokument muss zum organisatorisch frühestmöglichen Zeitpunkt archiviert werden können.	✓
4. Es ist gewährleistet, dass jedes Dokument mit seinem Original übereinstimmt und unveränderbar archiviert werden kann.	✓
5. Jedes Dokument darf bei Bedarf nur von entsprechend berechtigten Benutzern eingesehen werden.	✓
6. Jedes Dokument muss in angemessener Zeit wiedergefunden und reproduziert werden können.	✓
7. Jedes Dokument darf frühestens nach Ablauf seiner Aufbewahrungsfrist vernichtet, d.h. aus dem Archiv gelöscht werden.	✓
8. Jede ändernde Aktion im elektronischen Archivsystem muss für Berechtigte nachvollziehbar protokolliert werden.	✓
9. Das gesamte organisatorische und technische Verfahren der Archivierung kann von einem sachverständigen Dritten jederzeit geprüft werden.	✓
10. Bei allen Migrationen und Änderungen am Archivsystem muss die Einhaltung aller zuvor aufgeführten Grundsätze sichergestellt sein.	✓

IV. GFI Archiver 2015 - Sicherheit und Datenschutz als Teil der IT-Compliance

1. Grundlagen - IT-Sicherheit als Teil der IT-Compliance

(1) Der Schutz der IT-Infrastruktur ist eine zentrale Anforderung an die IT-Compliance. Jedes Unternehmen hat seine technische Infrastruktur unter Berücksichtigung des Stands der Technik gegen unerlaubten Zugriff oder Schädigung durch Dritte zu schützen.

(2) Vorstände und Geschäftsführer sind zur Gewährleistung der erforderlichen Datensicherheit verpflichtet sind. Dies geht sogar über den Bereich der personenbezogenen Daten hinaus. Vom Schutzumfang umfasst sind auch Unternehmensdaten, Geschäfts- und Kundeninformationen oder Betriebsgeheimnisse. So verlangt das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich" (KonTraG) die Einrichtung einer IT-Sicherheitsarchitektur. Gemäß §§ 91 Abs. 2, 93 Abs. 1 Satz 1 AktG[3] i. V. m. §§ 30, 130 OWiG hat der Vorstand „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten", damit „den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden". Zu diesen Maßnahmen zählt der Schutz der IT- und Datensicherheit und stellt damit eine zentrale Anforderung an die IT-Compliance (IT-Security) dar. Diese Pflicht trifft zunächst die Geschäftsleitung der verantwortlichen Stelle. Die Unternehmensleitung hat damit für ein entsprechendes Risikomanagementsystem zu sorgen, um u. a. bestandsgefährdende Entwicklungen frühzeitig zu erkennen. Auch die technischen und organisatorischen Maßnahmen in der Anlage zu § 9 BDSG enthalten Vorgaben.

(3) Daneben könnten auch IT-Verantwortliche oder Systemadministratoren betroffen sein, wenn fehlende Sicherheitsmaßnahmen bei der Nutzung der IT-Infrastruktur zu datenschutzrechtlichen Ordnungswidrigkeiten, strafbaren Urheberrechtsverletzungen wegen unkontrollierter Softwareinstallationen oder auch zur strafbaren Weitergabe von Know-How (§§ 17, 18 UWG) führen.

(4) Jedes Unternehmen hat damit seine technische Infrastruktur gegen unerlaubten Zugriff oder Schädigung durch Dritte zu schützen. Zu beachten ist, dass durch Schadprogramme auch der Verlust von geheimen Betriebs- und Geschäftsgeheimnissen oder Unternehmens-Know-how droht, was erhebliche wirtschaftliche oder imageschädigende Auswirkungen auf das Unternehmen haben kann. Insoweit zählt die Implementierung einer geeigneten IT, auch in Form eines entsprechenden Überwachungstools zur Identifizierung von IT-Schwachstellen im Unternehmen.

(5) Im Rahmen der Nutzung des „GFI Archiver 2015" sind die Grundprinzipien der IT-Sicherheit berücksichtigt und können damit vom Nutzer rechtskonform eingesetzt werden.

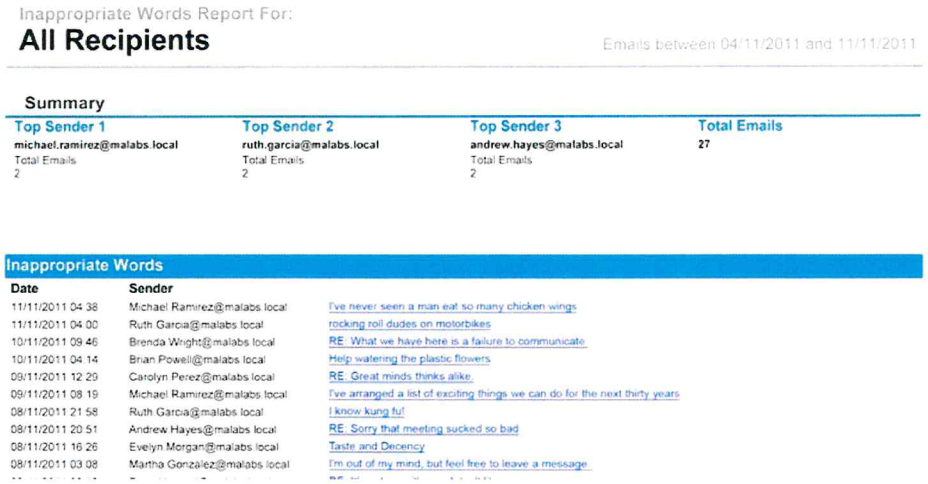
Anforderung Datensicherheit	
1. **Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle) - vom Nutzer umzusetzen.**	✓
2. **Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangs-kontrolle) - vom Nutzer umzusetzen.**	✓

3 Diese Verpflichtungen gelten gleichermaßen für Geschäftsführer einer GmbH sowie für die OHG und die KG, wenn sie keine natürliche Person als persönlich haftenden Gesellschafter hat (§§ 43 f. GmbHG). Schließlich besteht nach § 111 Abs. 1 AktG eine Überwachungspflicht des Aufsichtsrats gegenüber dem Vorstand in Bezug auf die Etablierung einer IT-Sicherheitsarchitektur. Sollten Geschäftsführer, Vorstände oder Aufsichtsräte ihre Pflichten zur IT-Security bzw. ihre diesbezügliche Überwachungspflicht verletzen, haften sie gegenüber ihrem Unternehmen persönlich.

3.	Der GFI Archiver 2015 gewährleistet, dass die zur Benutzung des Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen und, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).	✓
4.	Der GFI Archiver 2015 gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle).	✓
5.	Der GFI Archiver 2015 gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).	✓
6.	Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entspre-chend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle) - vom Nutzer um-zusetzen.	✓
7.	Der GFI Archiver 2015 gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle).	✓
8.	Der GFI Archiver 2015 gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).	✓

2. Datenschutz - IT-Sicherheit als Teil der IT-Compliance

(1) Neben den sicherheitsrelevanten Daten werden mittels des GFI Archiver 2015 auch personenbezogene Daten von Mitarbeitern erhoben und letztlich verarbeitet. Zumindest ist ein Rückgriff auf die Daten des Mitarbeiters mit Hilfe des GFI Archiver 2015 nicht ausgeschlossen.



Inappropriate Words Report For:

All Recipients

Emails between 04/11/2011 and 11/11/2011

Summary

Top Sender 1	Top Sender 2	Top Sender 3	Total Emails
michael.ramirez@malabs.local Total Emails 2	ruth.garcia@malabs.local Total Emails 2	andrew.hayes@malabs.local Total Emails 2	27

Inappropriate Words

Date	Sender	
11/11/2011 04:38	Michael.Ramirez@malabs.local	I've never seen a man eat so many chicken wings
11/11/2011 04:00	Ruth.Garcia@malabs.local	rocking roll dudes on motorbikes
10/11/2011 09:46	Brenda.Wright@malabs.local	RE: What we have here is a failure to communicate
10/11/2011 04:14	Brian.Powell@malabs.local	Help watering the plastic flowers
09/11/2011 12:29	Carolyn.Perez@malabs.local	RE: Great minds thinks alike.
09/11/2011 08:19	Michael.Ramirez@malabs.local	I've arranged a list of exciting things we can do for the next thirty years
08/11/2011 21:58	Ruth.Garcia@malabs.local	I know kung fu!
08/11/2011 20:51	Andrew.Hayes@malabs.local	RE: Sorry that meeting sucked so bad
08/11/2011 16:26	Evelyn.Morgan@malabs.local	Taste and Decency
08/11/2011 03:08	Martha.Gonzalez@malabs.local	I'm out of my mind, but feel free to leave a message

- Abbildung: 18 -

(2) Dies eröffnet den Anwendungsbereich des BDSG (§ 4 Abs. 1 BDSG).

(3) Bei der Überwachung des Nutzerverhaltens von Mitarbeitern, auch zur Vermeidung von IT-Sicherheitsrisiken, ist die seit Jahren kontrovers geführte Diskussion zu berücksichtigen, ob der Arbeitgeber im Falle der erlaubten Privatnutzung des Internets den Bestimmungen des Telekommunikations-rechts (TKG) unterfällt.

(4) Wenn man zu dem Schluss gelangt, dass das TKG nicht auf Arbeitgeber anzuwenden sei oder die private Nutzung der dienstlichen IT vollum-fänglich untersagt, bleibt die rechtliche Bewertung anhand der Vorgaben des Datenschutzrechts. Entgegen einer weit verbreiteten Ansicht ist auch in diesen Fällen eine unkontrollier-te Überwachung und Einsichtnahme in die Kommunikation des Mitarbeiters nicht zulässig. Auch hier ergeben sich juristische Hürden, die es zu beachten gilt.

(5) Die Zulässigkeit der Verarbeitung von Daten des Mitarbeiters richtet sich grundsätzlich nach § 32 Abs. 1 oder § 28 Abs. 1 S. 2 Nr. 2 BDSG. Welche dieser Bestimmungen einschlägig ist, hängt davon ab, welcher Zweck für den Arbeitgeber bei der Überprüfung betroffen ist. Liegt der Schwerpunkt der Auswertung auf dem Verhalten eines Mitarbeiters, kommt in der Regel § 32 BDSG zur Anwendung. Zweckbeispiele für § 28 Abs. 1 S. 1 Nr. 2 BDSG hingegen sind etwa die Untersuchung oder Behandlung von IT-Sicher-heitsvorfällen, die Einsichtnahme in zurückliegende Geschäftsvorfälle (z. B. im Rahmen von Gerichtsverfahren) oder interne Ermittlungen, beispielswei-se zu Straftaten anderer Arbeitnehmer. Beiden Ermächtigungsgrundlagen gemein ist das gesetzliche Gebot der Verhältnismäßigkeit. Dies wiederum erfordert für den Arbeitgeber im Falle eines Daten-zugriffs, in jedem Fall eine umfassende Abwägung sämtlicher betroffener Interessen beider Parteien im Einzelfall. Nur, wenn eine solche Abwägung zu Gunsten der In-teressen des Arbeitgebers ausfällt, ist die Maßnahme letztlich auch zulässig.

(6) Zu Gunsten des Arbeitnehmers zählen dabei stets das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung. Der Arbeitgeber hingegen kann sich auf das Eigentumsrecht, den Schutz des eingerichteten und ausgeübten Gewerbebetriebs sowie das Grundrecht auf Berufsfreiheit stützen. Er-gänzend muss der Arbeitgeber bei jeder Art der Datenverarbeitung stets auf die Einhaltung der Datenschutz-grundsätze achten, insbesondere in Form des Prinzips der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG). Sofern mit der Verarbeitung ein besonderes Risiko für die Rechte des Betroffenen i. S. von § 4 d Abs. 5 BDSG verbunden ist, kann zudem eine Vorabkontrolle durch den Datenschutzbeauftragten erforderlich sein.

(7) Unter Berücksichtigung der §§ 28 Abs. 1 S. 1 Nr. 2 und 32 BDSG können die gegenüberstehenden Interessen mit der vorliegenden Anwendung zu Gunsten des Arbeitgebers abgewogen werden. Eine unverhältnis-mäßige Beeinträchtigung der Interessen der Beschäftigten ist nicht erkennbar. Auch die übrigen daten-schutzrechtlichen Anforderungen können mit der Anwendung umgesetzt werden.

V. Mitbestimmungsrechte

(1) Beim Einsatz des GFI Archiver 2015 ist stets das Mitbestimmungsrecht des Betriebsrats gemäß § 87a Nr. 6 BetrVG zu beachten. Der Betriebsrat kann demnach mitbestimmen über die „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen".

(2) Erfasst werden daher grundsätzlich alle technischen Einrichtungen, die durch Beobachtung und Beaufsichtigung des Arbeitnehmers eine Information geben, die Rückschlüsse auf das Verhalten oder die Leistung der betroffenen Arbeitnehmer zulässt. Unerheblich ist, ob der Arbeitgeber mit dieser Einrichtung auch selbst den Zweck verfolgt, das Verhalten oder die Leistung des Arbeitnehmers zu überwachen. Vielmehr genügt es, dass die technische Einrichtung nach ihrer Konstruktion oder dem eingefügten Programm, zu einer Kontrolle bestimmt ist.

(3) Die Einbeziehung des Betriebsrates wird folglich empfohlen.

C. Fazit

C.
Fazit

Mittels des „GFI Archiver 2015" sind die rechtlichen Vorgaben an die Grundsätze zur ordnungsmäßigen Füh-rung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff erfüllt, bzw. können vom Nutzer rechtskonform umgesetzt und berücksichtigt werden. Auch im Hin-blick auf die Anforderungen an das Bundesdatenschutzgesetz entspricht das Programm den gesetzlichen Anforderungen.

D.
Rechtlicher Hinweis

D. Rechtlicher Hinweis

Wir weisen darauf hin, dass das vorliegende Gutachten mit größter Sorgfalt durchgeführt wurde und die Einschätzung auf unserer persönlichen rechtlichen Bewertung basiert. Ungeachtet dessen besteht bei derartigen Rechtsfragen und Begutachtungen stets die Möglichkeit einer anderen Auffassung, zumal höchstrichterliche Entscheidungen von Gerichten zu einer Vielzahl der aufgeworfenen Bereiche bislang fehlen. Zudem besteht bei derartigen Prüfungen grundsätzlich immer die Möglichkeit, dass sich die Rechtslage aufgrund von überar-beiteten Gesetzen, Verordnungen und Vereinbarungen verändert.

Dieser Prüfbericht stellt zudem keine Rechtsberatung dar und kann eine solche auch keinesfalls ersetzen. Wir empfehlen stets, sich bei informations- oder datenschutzrechtlichen Fragen von spezialisierten Rechtsanwälten individuell rechtlich beraten zu lassen.

GFI®

www.gfisoftware.de

Kontaktdaten aller GFI-Niederlassungen weltweit finden
Sie hier: www.gfisoftware.de/contact-us

Weitere Lösungen für E-mail und Messaging von GFI Software

GFI FaxMaker™
Netzwerk-Fax-Server-Software für Exchange/SMTP/Lotus

GFI FaxMaker™ Online
Online-Faxkommunikation – schnell und einfach

GFI MailEssentials®
E-Mail-Sicherheit und Spam-Abwehr für Exchange/SMTP/Lotus