

# Prüfungsbericht

**GFI MailArchiver™** 2011 R3

## MailInsights IT-Compliance Check 2012

Prüfung der MailInsights Funktionalitäten nach den Grundsätzen des Bundesdatenschutzgesetzes (BDSG) und des Betriebsverfassungsgesetz (BetrVG)



## Inhaltsverzeichnis

1. Prüfungsauftrag .....	2
2. Technische Grundlagen .....	3
3. Rechtliche Grundlagen .....	3
4. Datenschutz und Betriebsverfassungsrecht.....	3
5. Erkenntnisse und Empfehlungen aus der Prüfung.....	5
a. Kommunikationsfluss.....	5
b. WebMail Nutzung .....	7
c. Email Reaktionsverhalten .....	8
d. Unangemessene Wörter.....	9
e. Inaktive Konten .....	10
f. Speichernutzung.....	10
6. Ergebnisse zu den datenschutzrechtlichen Anforderungen.....	11
7. Anforderung des Betriebsverfassungsgesetzes an den Einsatz.....	12
8. Abschließende Empfehlung und Tipps .....	13

## 1. Prüfungsauftrag

Am 04. November 2011 wurden PRW RECHTSANWÄLTE von der

GFI Software Development Ltd.

San Andrea Street

San Gwann, MT SGN 1612 Malta (nachfolgend „GFI“)

mit der Prüfung der MailInsights Funktionalitäten im Produkt GFI MailArchiver 2011 R 3 hinsichtlich der Anforderungen nach den Grundsätzen des Bundesdatenschutzgesetzes (BDSG) und des Betriebsverfassungsgesetzes (BetrVG) beauftragt. Prüfungsgegenstand waren folgende Softwarelösungen:

- Kommunikationsfluss
- Webmail Nutzung
- Email Reaktionsverhalten
- Speichernutzung
- Inaktive Konten
- Unangemessene Wörter

Ziel der Prüfung war es somit festzustellen, ob bei der Nutzung der MailInsights Funktionalitäten die oben genannten gesetzlichen Anforderungen berücksichtigt werden können. Bei MailInsights handelt es sich im Wesentlichen um ein integriertes Berichtsmodul innerhalb des GFI MailArchiver 2011 R3, mithin eine Software, welche Berichte liefern kann.

Nicht gefordert waren Softwarebescheinigungen im Sinne des IDW-Prüfungsstandards „Erteilung und Verwendung von Softwarebescheinigungen“ (IDW PS 880). Die Verfahren der Softwareentwicklung waren nicht Gegenstand der Prüfungshandlungen. Hinweis: Eine vollumfängliche Prüfung des Produktes GFI MailArchiver wurde bereits im Jahre 2010 positiv durchgeführt. Hierauf wird verwiesen.

Die nachfolgenden Ausführungen erheben keinen Anspruch auf Vollständigkeit. Sie geben aber einen ersten Einblick in die sich noch entwickelnde Rechtsthematik IT-Compliance konformer Anwendung von IT-Lösungen. Berücksichtigt wurde hier ausschließlich die Rechtslage in Deutschland. Dieser Bericht gibt einen Überblick über eine Reihe von einzuhaltenden gesetzlichen Vorgaben sowie Tipps zu ihrer Umsetzung. Die Rechtsberatung im Einzelfall kann hierdurch jedoch nicht ersetzt werden. Insbesondere können im hier gewählten Umfang keine branchenmäßigen Besonderheiten abgebildet werden. Dieser Bericht greift die Rechtsthemen Datenschutz und Betriebsverfassungsgesetz im Zusammenhang mit der Nutzung von GFI MailArchiver 2011 R 3 MailInsights auf Administratorebene auf und soll Empfehlungen für eine rechtskonforme Nutzung von MailInsights aufzeigen.

Die Prüfungen wurden seitens GFI durch einen sehr fachkundigen Sales Engineer und seitens der PRW Consulting GmbH durch einen technischen IT-Compliance Beauftragten unterstützt.

Die Prüfungen wurden am 11.11.2011 abgeschlossen.

## 2. Technische Grundlagen

Die MailInsights Berichte können nicht anonymisiert ausgewertet werden. Benutzer, die Vollzugriffsrechte auf alle Mailarchive haben (berechtigte Benutzer), können die MailInsights Berichte mit allen persönlichen Daten (insb. Absender, Empfänger, Betreff) einsehen. Die nachfolgend rechtlich beschriebenen Funktionen von MailInsights können aktiviert oder nicht aktiviert werden. Ohne eine Aktivierung sind die nachfolgenden Ausführungen nicht relevant, da keine Reports, die gegebenenfalls gegen datenschutzrechtliche oder betriebsverfassungsrechtliche Anforderungen verstoßen, generiert werden können.

## 3. Rechtliche Grundlagen

Die rechtlichen Grundlagen der Prüfung ergeben sich aus nachfolgenden Normen:

- § 3a BDSG
- § 4 BDSG
- § 9 BDSG
- Anlage zu § 9 BDSG, Nummer 2
- Anlage zu § 9 BDSG, Nummer 3
- Anlage zu § 9 BDSG, Nummer 4
- Anlage zu § 9 BDSG, Nummer 5
- § 87 Abs. 1, Nummer 6 BetrVG

## 4. Datenschutz und Betriebsverfassungsrecht

Im Datenschutzrecht gilt der Grundsatz der Datenvermeidung und Datensparsamkeit.<sup>1</sup> Dies bedeutet, dass personenbezogene Daten nur unter strengen Voraussetzungen erhoben, verarbeitet und eben auch gespeichert werden dürfen. Das Arbeiten mit personenbezogenen Daten sollte begrenzt oder vermieden werden.

Regelungen im Bezug auf die Überwachung der PC-Tätigkeiten von Arbeitnehmern finden sich unter anderem in der Bildschirmarbeitsverordnung (BildscharbV) in Ziffer 22 des Anhangs zur Bildschirmarbeitsverordnung. Hier heißt es

*„Ohne Wissen der Benutzer darf keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden.“* Damit ist dem Arbeitgeber ein heimlicher Einsatz von Überwachungssoftware und -hardware untersagt.

Der Arbeitgeber ist nach § 87 BetrVG verpflichtet, die Zustimmung des Betriebsrats einzuholen, bevor er eine Maßnahme umsetzt, die dem Mitbestimmungsrecht des Betriebsrats unterliegt. Die Zustimmung des Betriebsrats stellt hierbei eine Wirksamkeitsvoraussetzung dar. Setzt der Arbeitgeber eine Maßnahme demnach einseitig um, ohne zuvor mit dem Betriebsrat eine Einigung erzielt zu haben, ist die Maßnahme rechtswidrig.

---

<sup>1</sup> § 3a BDSG

Als Sanktion gegen einen Verstoß gegen sein Mitbestimmungsrecht steht dem Betriebsrat gegen den Arbeitgeber ein Anspruch auf Beseitigung, wie auch auf Unterlassung zu. Sind arbeitnehmerbezogene Daten unrechtmäßig erhoben worden, steht den Betroffenen zudem ein Beseitigungs- und Unterlassungsanspruch wegen Treupflichtverletzung sowie Verletzung des Persönlichkeitsrechts, ggf. auch Schmerzensgeld, zu.<sup>2</sup> Daneben kann ein Verstoß strafrechtliche Sanktionen (z.B. §§ 201, 202a und 206 StGB) oder Bußgelder (§ 149 TKG) nach sich ziehen. Prozessual sind die unrechtmäßig gewonnenen Informationen gegen den Arbeitnehmer regelmäßig nicht verwertbar<sup>3</sup>.

§ 87 Abs. 1 Nr. 6 BetrVG befasst sich mit der Arbeitnehmerüberwachung durch sog. technische Einrichtungen und soll das Mitbestimmungsrecht des Betriebsrats sichern, um die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern.<sup>4</sup> Da der Einsatz technischer Kontrolleinrichtungen zu einer anonymen und damit für den Arbeitnehmer nicht erkennbaren und abwendbaren Überwachung führt und die durch die Überwachung gewonnenen Daten auf Dauer gespeichert und verarbeitet werden können, wird in besonderem Maße in den persönlichen Bereich der überwachten Arbeitnehmer eingegriffen.<sup>5</sup>

Durch das zwingende Mitbestimmungsrecht des Betriebsrats bei der Einführung und Anwendung technischer Überwachungseinrichtungen sollen die Arbeitnehmer des Betriebs vor rechtlich unzulässigen Eingriffen in ihr Persönlichkeitsrecht geschützt und zugleich rechtlich zulässige Überwachungsmaßnahmen auf das unbedingt erforderliche Maß beschränkt werden.

Um die Gefahren, die dem Arbeitnehmer durch die modernen Technologien mit ihren vielfältigen, oft nicht wahrnehmbaren Überwachungsmöglichkeiten drohen, wirksam eindämmen zu können, bedarf der individualrechtliche Persönlichkeitsschutz der kollektiv-rechtlichen Verstärkung durch die Mitbestimmung.<sup>6</sup>

Die Einführung technischer Einrichtungen, wie eines Datenverarbeitungssystems, die das Verhalten oder die Leistung der Arbeitnehmer überwachen können, unterliegt der Mitbestimmung des Betriebsrats (§ 87 Abs. 1 Nr. 6 BetrVG). Betriebsvereinbarungen können aber nach Auffassung des Bundesarbeitsgerichts, die Zulässigkeit der Verarbeitung personenbezogener Daten abweichend von den gesetzlichen Vorschriften regeln. Die Grenze wird dann aber dort zu ziehen sein, wo die Personaldatenverarbeitung nach dem Bundesdatenschutzgesetz unzulässig ist.<sup>7</sup>

<sup>2</sup> Kraft/Wiese, Gemeinschaftskommentar zum Betriebsverfassungsgesetz, 2. Bd., 2005, § 87, Rdnr. 581.

<sup>3</sup> BAG, Urteil vom 29.10.1997 - 5 AZR 508/96, NZA 1998, 307 f.

<sup>4</sup> Analoge Vorschriften existieren auch für den öffentlichen oder kirchlichen Rechtsraum; im öffentlichen Dienst des Personalrats, vgl. § 75 Abs. 3 Nr. 17 BPersVG.

<sup>5</sup> vgl. BT-Drs VI/1786 S.49.

<sup>6</sup> BetrVG – Fitting, Handkommentar 25. Aufl., Rdnr. 215 zu § 87 BetrVG.

<sup>7</sup> Vergleiche Gola/Schomerus, BDSG § 4, Rdnr. 6.

## 5. Erkenntnisse und Empfehlungen aus der Prüfung

### a. Kommunikationsfluss

Dieser Bericht zeigt auf, welche User oder User Gruppen intern oder extern kommunizieren. Die Anwendung zeigt die gesamte interne und externe Email-Kommunikation auf.

Kommunikationsflussbericht für: **Administrator** Top 20-Benutzer  
 E-Mails zwischen 01.09.2011 und 04.11.2011

---

**Übersicht**

Kontakte gesamt	Intern insgesamt	Top intern	Extern insgesamt	Top extern
6 100 % von Kontakten gesamt	1 16 % von Kontakten gesamt	Finance 2	5 83 % von Kontakten gesamt	test@test.com 24



**Hinweis:**  
 ● Der Knotendurchmesser gibt die Häufigkeit der E-Mail-Kommunikation an.  
 Die Farbe zeigt die gleiche E-Mail-Domäne an.

Kommunikationsfluss					
Kontakt-E-Mail	Gesendete E-Mails	Empfangene E-Mails	E-Mails insgesamt	Letzte Kommunikation	
● test@test.com	0	24	24	26.10.2011 02:15	
● a@b.com	0	22	22	26.10.2011 02:16	
● c@a.com	0	10	10	26.10.2011 02:16	
● e@a.com	0	10	10	26.10.2011 02:16	
● b@a.com	0	10	10	26.10.2011 02:16	
● finance@gfi.local	2	0	2	26.10.2011 04:12	

Abbildung 1: Screenshot Kommunikationsfluss

#### (1) Datenschutz

Ein wesentlicher Grundsatz des Bundesdatenschutzgesetzes ist das so genannte Verbotsprinzip mit Erlaubnisvorbehalt (§ 4 BDSG). Dieses besagt, dass die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten verboten ist. Sie ist nur dann erlaubt, wenn entweder eine klare Rechtsgrundlage gegeben ist oder wenn die betroffene Person ausdrücklich (meist schriftlich) ihre Zustimmung zur Erhebung, Verarbeitung und Nutzung gegeben hat (§ 13 Abs. 2 ff. BDSG). Die angewendeten Verfahren mit

automatisierter Verarbeitung sind vom Datenschutzbeauftragten zu prüfen, oder (wenn ein solcher nicht vorhanden ist) bei der zuständigen Aufsichtsbehörde anzeigepflichtig (§ 4d BDSG).

Voraussetzung für die Anwendung dieser Funktionalität ist somit, dass es im Anwendungsbereich eine Regelung gibt, die einen solchen Bericht erlaubt. Zwar könnte argumentiert werden, dass dieser Bericht ausschließlich darüber informiert, wer kommuniziert und nicht darüber berichtet, mit wem und welchen Inhalt. Bei korrekter Auslegung des Datenschutzes lässt sich aber zumindest aus den Berichten ableiten, wer kommuniziert. Daten sind personenbezogen und damit geschützt, wenn sie persönliche oder sachliche Verhältnisse einer natürlichen Person beschreiben. Dazu genügt es, wenn die Person nicht namentlich benannt wird, aber bestimmbar ist (beispielsweise: Telefonnummer, Email-Adresse, IP-Adresse beim Surfen, Personalnummer). Also schon nach dem Datenschutzgesetz würde eine rechtliche Hürde bestehen.

## (2) Betriebsverfassungsrecht

In betriebsverfassungsrechtlicher Hinsicht sind vom Mitbestimmungstatbestand des § 87 Abs. 1 Nr. 6 BetrVG nur solche Überwachungsmaßnahmen erfasst, die mit Hilfe technischer Einrichtungen durchgeführt werden. Durch den Einsatz der technischen Überwachungseinrichtung müssen Daten erhoben werden, die Rückschlüsse auf das Verhalten bzw. die Leistung der Arbeitnehmer zulassen.<sup>8</sup>

Bei dem Produkt GFI MailArchiver 2011 R 3 bzw. deren MailInsights Funktionalitäten handelt es sich um eine solche technische Einrichtung, da der Einsatz auf Grund der technischen Gegebenheiten (bzw. siehe oben Ziff. 2 „Technische Grundlagen“) des Programms und der konkreten Art ihrer Verwendung objektiv geeignet<sup>9</sup> ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen und die Anwendung in der jeweiligen Funktionalität auch eine eigenständige Kontrollwirkung haben kann.

Bei der vorgenannten Anwendung kann auch die Überwachung des Verhaltens oder der Leistung des Arbeitnehmers vorgenommen werden, welche § 87 Abs. 1 Nr. 6 BetrVG fordert. Nach der Rechtsprechung des Bundesarbeitsgerichts<sup>10</sup> (BAG) liegt eine Überwachung i. S. d. § 87 Abs. 1 Nr. 6 BetrVG vor, wenn durch den Einsatz der technischen Einrichtungen Informationen über das Verhalten oder die Leistung der Arbeitnehmer erhoben und aufgezeichnet werden, damit diese der menschlichen Wahrnehmung zugänglich gemacht werden. So kann im hier untersuchten Bereich „Kommunikationsfluss“ festgestellt werden, welcher Mitarbeiter mit wem und zu welcher Zeit per Email kommuniziert hat. Der berechtigte Benutzer kann der Anwendung entnehmen, welcher Mitarbeiter Emails verschickt und erhalten hat und wann die letzte Kommunikation stattgefunden hat.

Vor diesem Hintergrund besteht für den Einsatz der hier genannten Funktion (Kommunikationsfluss) das Erfordernis der Zustimmung durch den Betriebsrat (§ 87 Abs. 1 Nr. 6 BetrVG).

<sup>8</sup> Richardi, in: Richardi, Betriebsverfassungsgesetz, 12. Aufl. 2010, § 87, Rdnr. 90.

<sup>9</sup> BetrVG – Fitting, Handkommentar, a.a.O. § 87, Rdnr. 226.

<sup>10</sup> BAG, Beschluss vom 14.09.1984 - 1 ABR 23/82, NZA 1985, 28 ff.

## b. WebMail Nutzung

Dieser Bericht zeigt auf, welcher Mitarbeiter welche Email-Kommunikation mit internetbasierenden Email-Diensten durchführt. Die Intension für diesen Bericht ist es, einen ungewollten Datenabfluss zu ermitteln. Der Bericht bietet die Möglichkeit, die Kommunikation mit internetbasierenden Email-Diensten benutzerspezifisch aufzuzeigen. Auch die jeweiligen Zeiten, in denen die Kommunikation mit internetbasierenden Diensten durchgeführt wurde, wird nach Datum sortiert dargestellt.

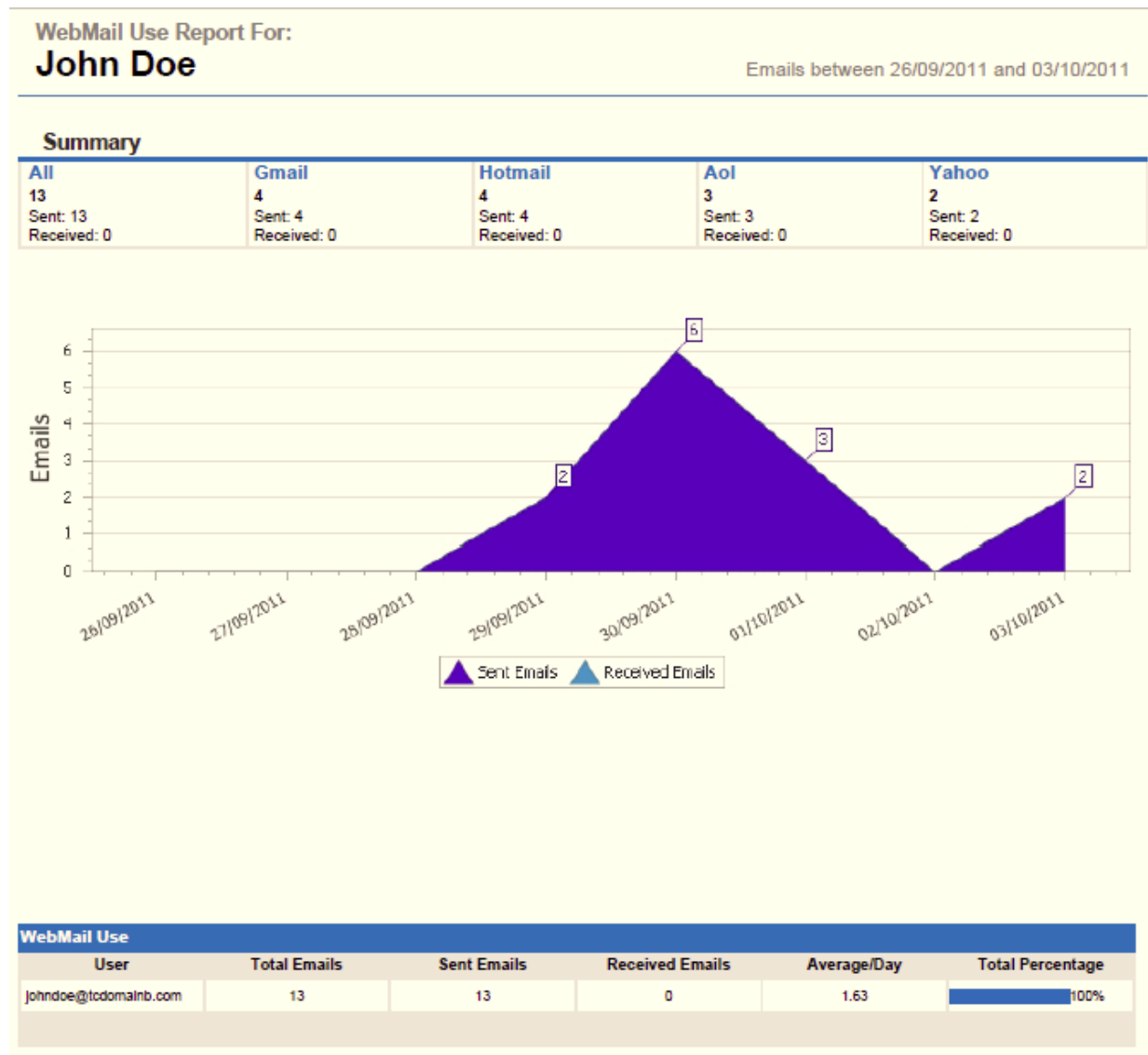


Abbildung 2: Screenshot WebMail Nutzung

### (1) Datenschutz

Hier kann auf 5. a) (1) verwiesen werden. Danach ist diese Auswertung vom BDSG nicht gedeckt und bedarf einer besonderen Erlaubnis.

## (2) Betriebsverfassungsrecht

Im Hinblick auf die betriebsverfassungsrechtlichen Vorgaben kann auf die oben gemachten Ausführungen verwiesen werden. Auch hier handelt es sich um eine explizit technische Einrichtung, mit der das Verhalten des Arbeitnehmers überwacht werden kann. Die Anwendung „WebMail Nutzung“ lässt direkte Rückschlüsse zu, welcher Mitarbeiter zu welchem Zeitpunkt mit einem bestimmten Mail-Anbieter bzw. dessen Kunden kommuniziert. Soweit auf diese Anwendung abzustellen ist, bedarf es ebenfalls der Zustimmung des Betriebsrates (§ 87 Abs. 1 Nr. 6 BetrVG).

## c. Email Reaktionsverhalten

Mit der Anwendung „Email Reaktionsverhalten“ kann ausgewertet werden, innerhalb welcher Zeiten der jeweilige Mitarbeiter auf Anfragen oder Mitteilung per Email reagiert und hierauf antwortet.

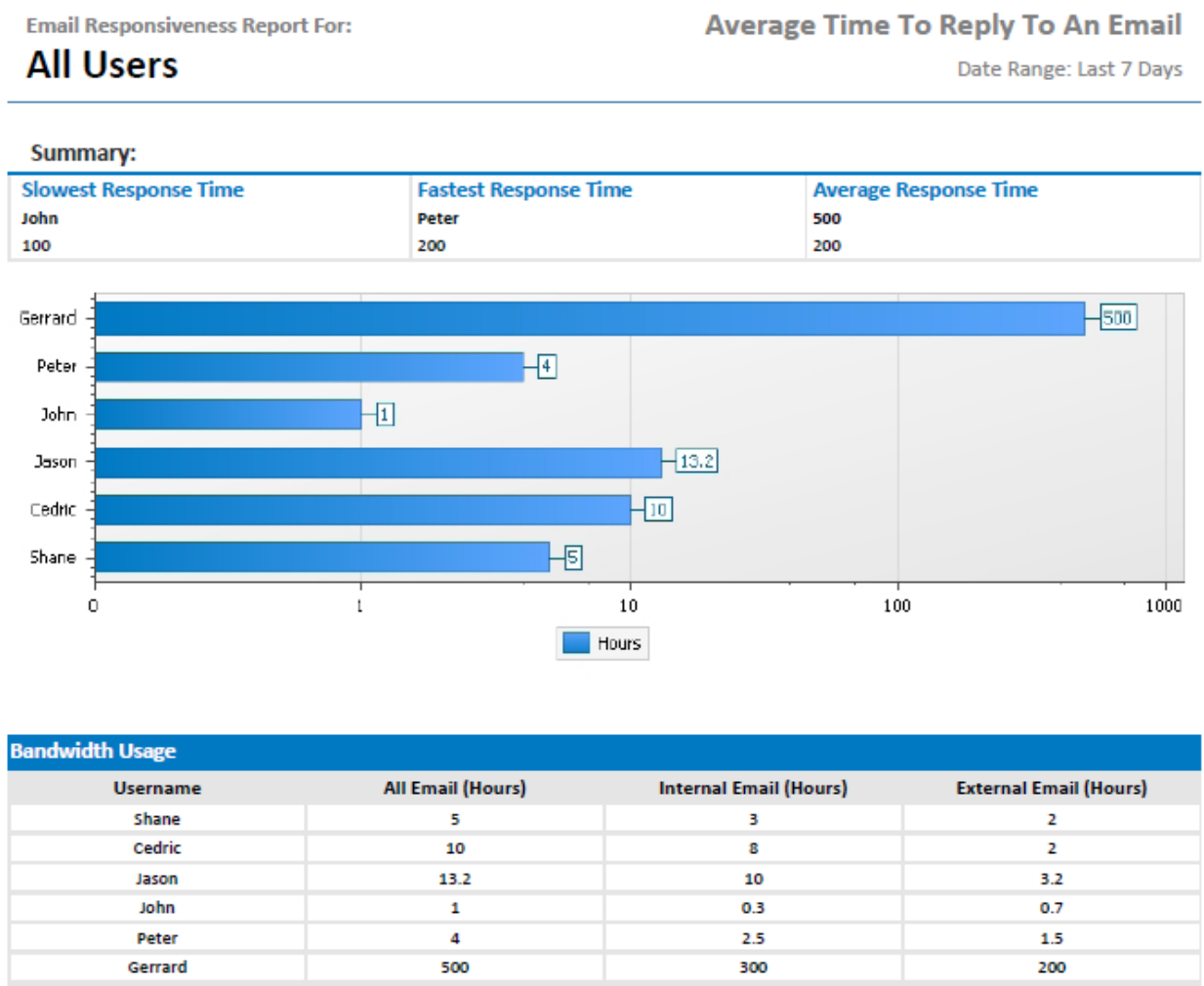


Abbildung 3: Screenshot Email Reaktionsverhalten

(1) **Datenschutz**

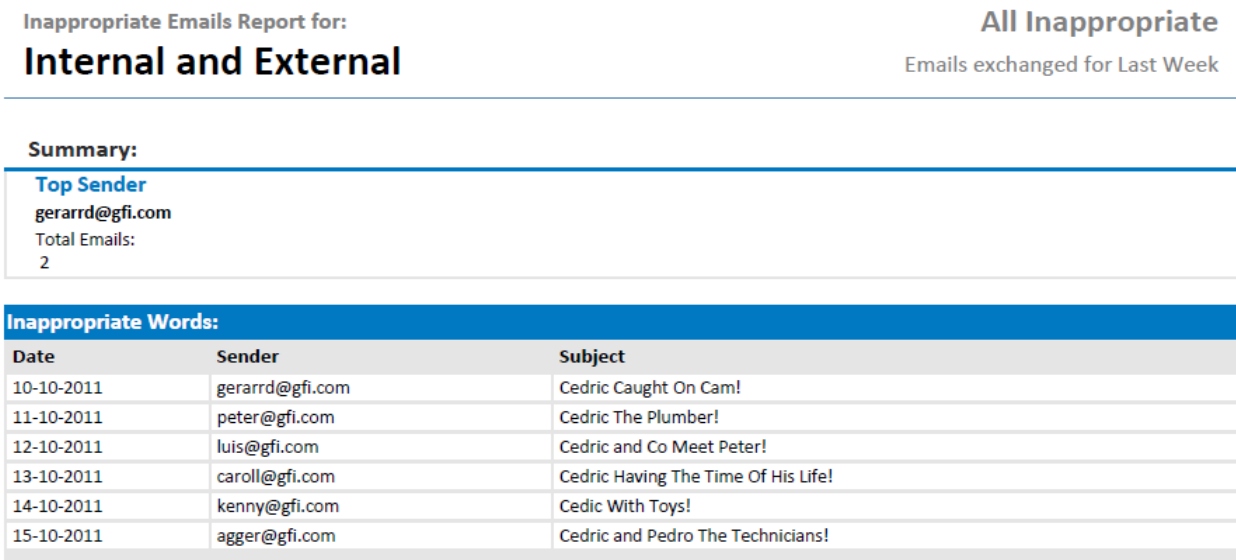
Hier kann auf 5. a) (1) verwiesen werden. Danach ist diese Auswertung vom BDSG nicht gedeckt und bedarf einer besonderen Erlaubnis.

(2) **Betriebsverfassungsrecht**

Auch bei dieser Anwendung sind die Voraussetzungen für eine Zustimmung durch den Betriebsrat erfüllt, da auch hier eine Überwachung der Mitarbeiter bzw. Arbeitnehmer möglich ist. Inhaltlich kann daher wiederum auf die vorgenannten Ausführungen verwiesen werden.

**d. Unangemessene Wörter**

Bei dem Bericht „unangemessene Wörter“ ist es dem jeweils berechtigten Benutzer möglich, nicht nur einen Filter für die Verwendung von bestimmten Wörtern in Emails einzurichten, um auf diese Weise herauszufinden, welcher Mitarbeiter unter Umständen ungewünschte Begriffe oder Begriffskombinationen im Rahmen seiner dienstlichen Kommunikation verwendet. Der berechtigte Benutzer kann auch die Angaben im „Betreff-Feld“ einsehen und möglicherweise herauslesen, welchen Inhalt die Email des Absenders hat.



**Inappropriate Emails Report for:** **Internal and External** **All Inappropriate**  
Emails exchanged for Last Week

---

**Summary:**

<b>Top Sender</b> gerarrd@gfi.com Total Emails: 2
--

**Inappropriate Words:**

Date	Sender	Subject
10-10-2011	gerarrd@gfi.com	Cedric Caught On Cam!
11-10-2011	peter@gfi.com	Cedric The Plumber!
12-10-2011	luis@gfi.com	Cedric and Co Meet Peter!
13-10-2011	caroll@gfi.com	Cedric Having The Time Of His Life!
14-10-2011	kenny@gfi.com	Cedric With Toys!
15-10-2011	agger@gfi.com	Cedric and Pedro The Technicians!

Abbildung4: Screenshot Unangemessene Wörter

(1) **Datenschutz**

Hier kann auf 5. a) (1) verwiesen werden. Danach ist diese Auswertung vom BDSG nicht gedeckt und bedarf einer besonderen Erlaubnis.

(2) **Betriebsverfassungsrecht**

Auch diese Anwendung fällt unter den Anwendungsbereich des Betriebsverfassungsrechts und bedarf der Zustimmung des Betriebsrates. Diese Anwendung stellt eine Überwachungsmöglichkeit des Mitarbeiters dar. Inhaltlich kann ebenfalls auf die zuvor gemachten Ausführungen verwiesen werden.

## e. Inaktive Konten

Bei dem Bericht „inaktive Konten“ werden alle inaktiven Benutzer aufgezeigt, welche in einem definierten Zeitraum keine Email Kommunikation (z. B. über einen Zeitraum von 180 Tagen) betrieben haben. Hierbei sind sowohl die Emails des jeweiligen Nutzers, als auch die Email-Adresse für den berechtigten Benutzer einsehbar.

Inactive User Report for all:  
**Internal Users**

**All Inactive Users**  
reported for the Last 30 Days

Inactive Users	
<b>Active Users</b> <b>500</b> % of all users: 50%	<b>Inactive Users</b> <b>500</b> % of all emails: 50%
User	Last Email Sent
user1@company.com	10/09/2011 11:00 am
user2@company.com	11/09/2011 09:30 am
user1@gmail.com	13/09/2011 03:30 pm
1-3 of 3	

Abbildung 5: Screenshot Inaktive Konten

### (1) Datenschutz

Hier kann auf 5. a) (1) verwiesen werden. Danach ist diese Auswertung vom BDSG nicht gedeckt und bedarf einer besonderen Erlaubnis.

### (2) Betriebsverfassungsrecht

Auch bei diesem Bericht sind betriebsverfassungsrechtliche Vorgaben zu beachten. Inhaltlich kann auf die vorgenannten Ausführungen zum Betriebsverfassungsrecht verwiesen werden

## f. Speichernutzung

Der Bericht über die Speichernutzung ermöglicht dem berechtigten Benutzer die Auswertung, welche Art von Emails versendet bzw. empfangen wird. Hierzu zählt einerseits die statistische Bewertung der Email-Größe sowie andererseits der angehangenen Dateitypen (Bilder, Videos, Dokumente usw.). Die Auswertung ist einerseits global für alle Mitarbeiter möglich, kann jedoch auch in seinem Zeitraum und der Benutzer angepasst werden. Durch diesen Bericht ist es möglich, Archivierungsregeln nachträglich einzurichten, die z. B. alle Emails mit Videoanhang oder – Inhalt verwirft, da dies nur „unnötig“ das Archiv vergrößert und belastet. Dadurch kann mit diesem Bericht die Speicherplatznutzung reduziert werden.

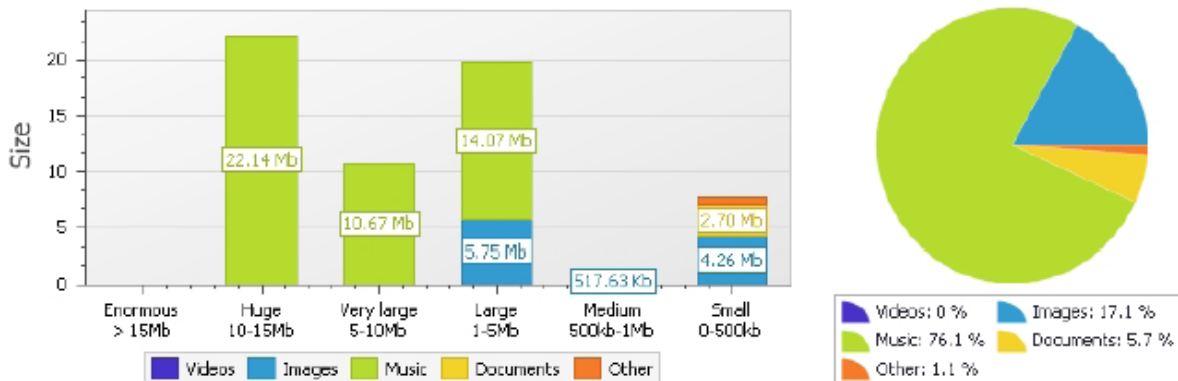
Auch ist es möglich, durch andere Filtermaßnahmen und Programme (z.B. Content-Filter für Emails) gewisse Dateitypen zu blockieren, so dass u.a. der Versand von Musikdateien nicht ermöglicht wird.

Storage Use Report For:  
**Everyone**

**Sent And Received Emails**  
Emails between 4/1/2011 and 9/26/2011

**Summary**

<b>Top Storage Type</b> Music - 46.88 Mb	<b>Bottom Storage Type</b> Other - 717.62 Kb	<b>Top Date</b> 9/15/2011 - 51.39 Mb
---	---	---



Storage Use:						
Date	Total Size	Videos Size	Images Size	Music Size	Documents Size	Other Size
9/16/2011	10.23 Mb	0 Mb	10.22 Mb	0 Mb	0 Mb	0.98 kb
9/15/2011	51.39 Mb	0 Mb	296.14 kb	46.88 Mb	3.52 Mb	716.63 kb

Abbildung 6: Screenshot Speichernutzung

**(1) Datenschutz**

Hier kann auf 5. a) (1) verwiesen werden. Danach ist diese Auswertung vom BDSG nicht gedeckt und bedarf einer besonderen Erlaubnis.

**(2) Betriebsverfassungsrecht**

Auch für die betriebsverfassungsrechtliche Bewertung kann auf die Ausführungen in 5 a) (2) verwiesen werden.

**6. Ergebnisse zu den datenschutzrechtlichen Anforderungen**

Wenn die Frage zur Zulässigkeit der Überwachung geklärt ist, sollten aber die weiteren Anforderungen des BDSG und seiner Anlage nicht außer Acht gelassen werden. Die GFI MailArchiver MaillInsights Funktion selbst hat keine „Funktionalität“ für den Datenschutz. Es besteht aber - wie dargestellt - die Möglichkeit und es liegt in der Hand des jeweiligen Unternehmens, durch geeignete technische und organisatorische Maßnahmen die Einhaltung der Datenschutzgesetze sicherzustellen.

Da mit der Software personenbezogene Daten erhoben beziehungsweise verwendet werden, sind einige Maßnahmen gemäß der Anlage zu § 9 BDSG zu treffen:

1. Die unautorisierte Benutzung der Software ist zu verhindern (Zugangskontrolle). Durch eine Zugangskontrollliste, kann die Benutzung des GFI MailInsights eingeschränkt werden. Man beachte hier auch die Führung einer Zugangskontrolle der Datenbank und des Betriebssystems des jeweiligen Servers.
2. Benutzer sollten lediglich auf die Daten Zugriff erhalten, für die sie auch befugt sind (Zugriffskontrolle). Es ist eine Unterscheidung nach einzelnen Berechtigungen konfigurierbar. Es wird empfohlen, ein rollenbasiertes Berechtigungskonzept zu implementieren, um den Zugriff auf Daten zu regeln.
3. Die Übermittlung von personenbezogenen Daten ist so abzusichern, dass während Datenübertragungen keine unbefugten Kopien, Veränderungen oder Löschungen der Daten getätigt werden können (Weitergabekontrolle). Auch hierzu wäre ein rollenbasiertes Berechtigungskonzept wünschenswert.
4. Es ist zu gewährleisten, dass die Eingabe, Änderung und Löschung von personenbezogenen Daten nachträglich nachvollziehbar ist (Eingabekontrolle).

Zusätzlich zu den oben genannten Maßnahmen ist eine Verwendung von Verschlüsselungsverfahren entsprechend dem Stand der Technik zu empfehlen.

## **7. Anforderung des Betriebsverfassungsgesetzes an den Einsatz**

Der Betriebsrat hat bei der Einführung und Anwendung technischer Überwachungseinrichtungen, mithin bei der Entscheidung über das „ob“ und das „wie“ des Einsatzes von GFI MailArchiver 2011 R 3 mitzubestimmen.

Die Einführung einer Software, mit derer das Verhalten oder die Leistung der Arbeitnehmer überwacht werden kann, unterliegt zwingend der Mitbestimmung des Betriebsrats (§ 87 Abs. 1 Nr. 6 BetrVG). Mit Hilfe des GFI MailInsights kann das Verhalten der Email-Nutzung von Mitarbeitern überwacht werden. In Betrachtung dieser Verwendungsmöglichkeit ist für die Einführung eines aktiven GFI MailInsights die Mitbestimmung des Betriebsrats erforderlich gemäß § 87 Abs. 1 Nr. 6 BetrVG.

Die Durchführung der betrieblichen Mitbestimmung an sich bedarf keiner besonderen Form, kann somit auch durch eine einfache Betriebsabsprache oder durch den Abschluss von Betriebsvereinbarungen erfolgen.

Betriebsvereinbarungen können arbeitgeberseitige Kontrollrechte und -maßnahmen allerdings nur im Rahmen der bestehenden Gesetze näher bestimmen. Eine darüber hinausgehende inhaltliche Kommunikationskontrolle kann durch Betriebsvereinbarungen nicht festgeschrieben werden, da es sich hierbei um Eingriffe in höchstpersönliche Rechtsgüter handelt, die nicht zur kollektiven, sondern allenfalls zur individuellen Disposition stehen. Überwachungsmaßnahmen sollten idealerweise nach Art und Umfang gem. §§ 94 ff. TKG, § 4a BDSG individuell, schriftlich und vorab mit dem Mitarbeiter vereinbart werden. Selbst wenn entsprechende

Einwilligungen der Mitarbeiter vorliegen, muss jedoch der Kernbereich der Persönlichkeitsrechte gewahrt werden und Kontrollen sind auf das Vorliegen bestimmter Verdachtsmomente zu reduzieren.

## 8. Abschließende Empfehlung und Tipps

Da keine gesetzliche Erlaubnisnorm zum Einsatz des GFI MailArchiver R3 MailInsights Funktion vorliegt, kann eine Zulässigkeit der Verwendung in Deutschland durch eine Individualvereinbarung im Arbeitsvertrag, durch eine Betriebsvereinbarung oder durch eine sog. Dienstanweisung (Policy) erreicht werden, in der das Verfahren beschrieben und rechtskonform gestaltet abgebildet wird. Es empfiehlt sich somit, detaillierte Regelungen betriebsbezogen und konkret auf die Verhältnisse im Unternehmen festzuhalten.<sup>11</sup> Inhalte könnten z.B. sein:

- Welche Daten dürfen überhaupt erhoben werden?
- Wer hat Zugriff auf diese Daten?
- Wie lange dürfen sie gespeichert werden?
- Wer darf sie zu welchem Zwecke und wofür verwenden?

Der Datenschutz und dort insbesondere der Mitarbeiterdatenschutz haben in Deutschland einen hohen Stellenwert. Dies ist bei der Abwägung der Sicherheitsinteressen der Unternehmen angemessen zu berücksichtigen. Solange ein neues Gesetz zum Arbeitnehmerdatenschutz ausbleibt, werden viele Regeln durch Gerichte nach dem Grundsatz der Verhältnismäßigkeit beschlossen und damit im Einzelfall bestimmt.

Da die Gesetze den Datenschutz im Arbeitsverhältnis nur sehr lückenhaft regeln und nicht alle Details durch Betriebsvereinbarungen geklärt sind, werden viele Fragen von den Arbeitsgerichten entschieden. Zu nennen sind beispielsweise die Grundsatzurteile des Bundesverfassungsgerichts (1 BvR 1611/96 vom 9. Oktober 2002) zum rechtswidrigen Mithören nicht-öffentlicher Kommunikation und des Bundesarbeitsgerichts zur Videoüberwachung am Arbeitsplatz (1 ABR 16/07 vom 26. August 2008) und zum Mithören von dienstlichen Telefongesprächen (6 AZR 189/08 vom 23. April 2009). Mittlerweile hat dieses so genannte Richterrecht für den Arbeitnehmerdatenschutz größere Bedeutung als die gesetzlichen Regelungen.

---

<sup>11</sup> <http://www.betriebsratsberater-berlin.de/betriebsratsberater-abc/betriebsratsberater-abc/datenschutz/mitbestimmung-des-betriebsrats-nach-87-abs-1-nr-6-betrvg.html>.