Juristisches Gutachten zu den technischen und organisatorischen Maßnahmen des Dienstes:

„Aeternum – das Hornetsecurity E-Mail-Archiv“

Rechtsanwalt Karsten U. Bartels LL.M., Berlin, 05.08.2015

I. PRÜFUNGSGEGENSTAND

Gegenstand der folgenden Prüfung ist die oben genannte Plattform und die dafür erforderliche IT-Struktur. Anbieter der Plattform ist die Hornetsecurity GmbH, Am Listholze 78, 30177 Hannover (folgend: Hornetsecurity).

Es war zu prüfen, ob und inwiefern die getroffenen IT-Sicherheitsmaßnahmen folgenden Anforderungen entsprechen:

- Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD), hinsichtlich Ziffer 3, 7 und 9 GoBD, einschließlich damit verbundener Anforderungen aus dem Handelsgesetzbuch (HGB) und
- § 9 Bundesdatenschutzgesetz (BDSG).

II. PRÜFUNGSERGEBNIS

Die unten beschriebenen technischen und organisatorischen Maßnahmen sowie die Verfahrensbeschreibung erfüllen das nach Ziffer 3, 7 und 9 GoBD sowie das nach § 9 BDSG erforderliche Niveau.

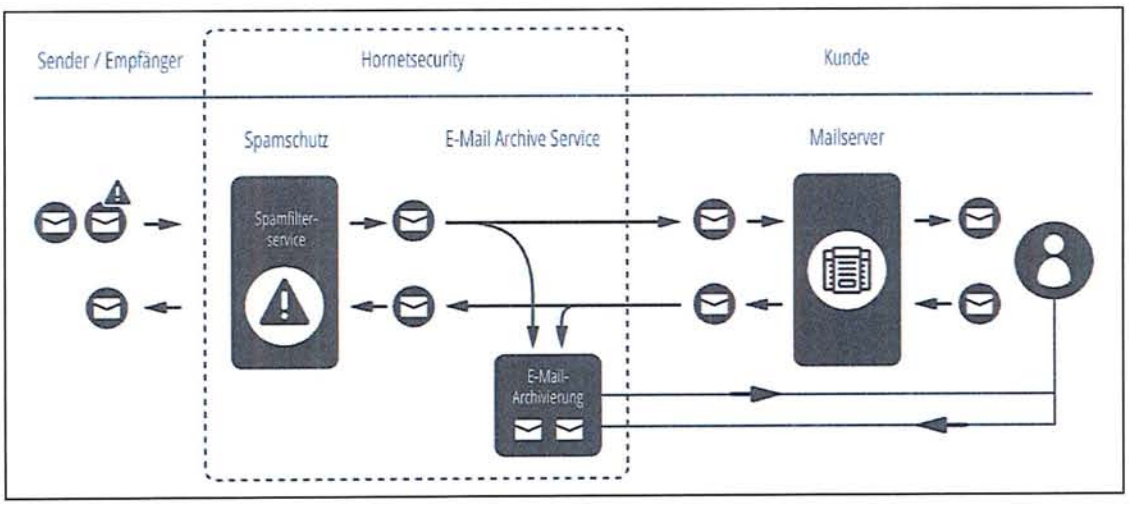
III. VERFAHRENSBESCHREIBUNG

Aeternum ist eine cloudbasierte E-Mail-Archivierungslösung von Hornetsecurity, um geschäftliche E-Mails sowohl aus dem Posteingang, als auch aus dem Pausausgang, gesondert speichern zu können.

1. Speicherungsverfahren

Von jeder E-Mail, gleich, ob ein- oder ausgehend, fertigt Aeternum eine Kopie an, die anschließend auf den Servern von Hornetsecurity gespeichert wird – unverändert und unveränderbar. Dies geschieht völlig automatisch und ohne Eingreifen von Administratoren oder Hornetsecurity.

Nähere Informationen zum E-Mail-Flow sind der Abbildung zu entnehmen:



Aeternum archiviert E-Mails, die mit externen Kommunikationspartnern ausgetauscht werden, bereits im Rahmen des ein- und ausgehenden SMTP-Versands vollständig. Alle E-Mails werden exakt so im Archiv gespeichert, wie sie die Gateways bzw. Relays von Hornetsecurity erreichen. Externe E-Mails sind dabei solche E-Mails, die nicht direkt den Domains zuzuordnen sind, die vom Mailserver des Kunden selber bedient werden. Externe E-Mails erreichen den Kunden grundsätzlich von außen durch das Internet per SMTP bzw. werden per SMTP zu einem anderen Mailserver übertragen (externes Routing). Ausgehende E-Mails werden vom Mailserver des Kunden an die Mail-Relays von Hornetsecurity geleitet und erst von dort dem Empfänger zugestellt. Eine Kopie der zugestellten E-Mail wird vom Mail-Relay im E-Mail-Archiv gespeichert. Auch hier ist sichergestellt, dass die E-Mail exakt so, wie sie dem Empfänger zugeschickt wurde, im Archiv gespeichert wird.

Die Speicherung der archivierten E-Mails erfolgt in Datenbanken. Gespeichert werden Header-Informationen (Absender, Empfänger, Betreff, Datum) sowie ein Volltextindex in einer No-SQL Datenbank und die komplette E-Mail „so wie sie ist" kundenbasiert in einer SQL Datenbank. Die Speicherung der Daten der Datenbanken erfolgt auf Festplatten mit RAID Level 5 oder 6.

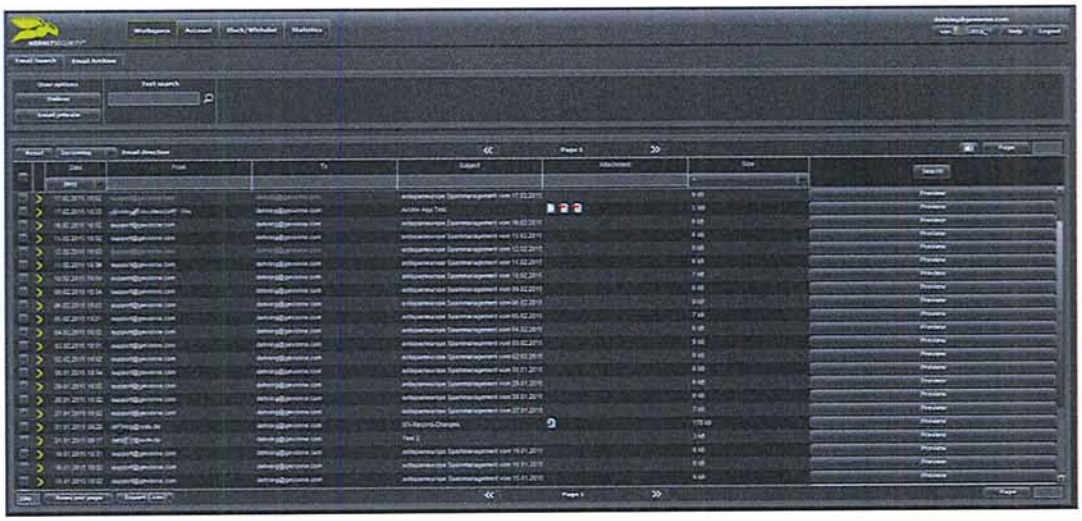
Die Veränderung von einmal im Archiv gespeicherten Daten durch Kunden ist außerdem technisch ausgeschlossen. Einmal im Archiv gespeicherte Daten können auch erst nach Ablauf der eingestellten Archivierungsfrist gelöscht werden. Nach Ablauf der Archivierungsfrist erfolgt die Löschung der Archivdaten automatisch.

Die Leistung erfolgt über mehrere, alle in Deutschland befindliche, Rechenzentren. Die von Hornetsecurity in den Rechenzentren betriebenen Systeme sind untereinander redundant, d.h. bei Ausfall eines einzelnen Systems, wird die Leistung durch andere Systeme übernommen. Weder der Ausfall einzelner Systeme, noch der eines kompletten Rechenzentrums führen zur Unterbrechung des E-Mail-Verkehrs.

2. Zugriff auf das E-Mailarchiv

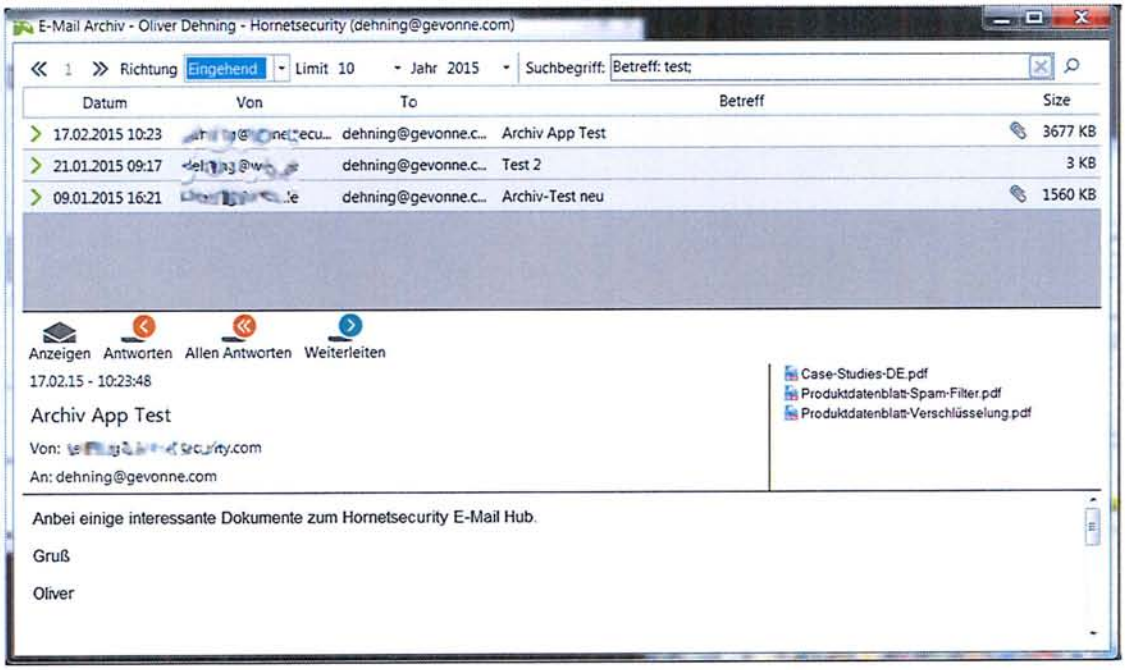
Auf in Aeternum gespeicherte Daten können autorisierte Benutzer über drei verschiedene Interfaces zugreifen:

- Hornetsecurity Control Panel

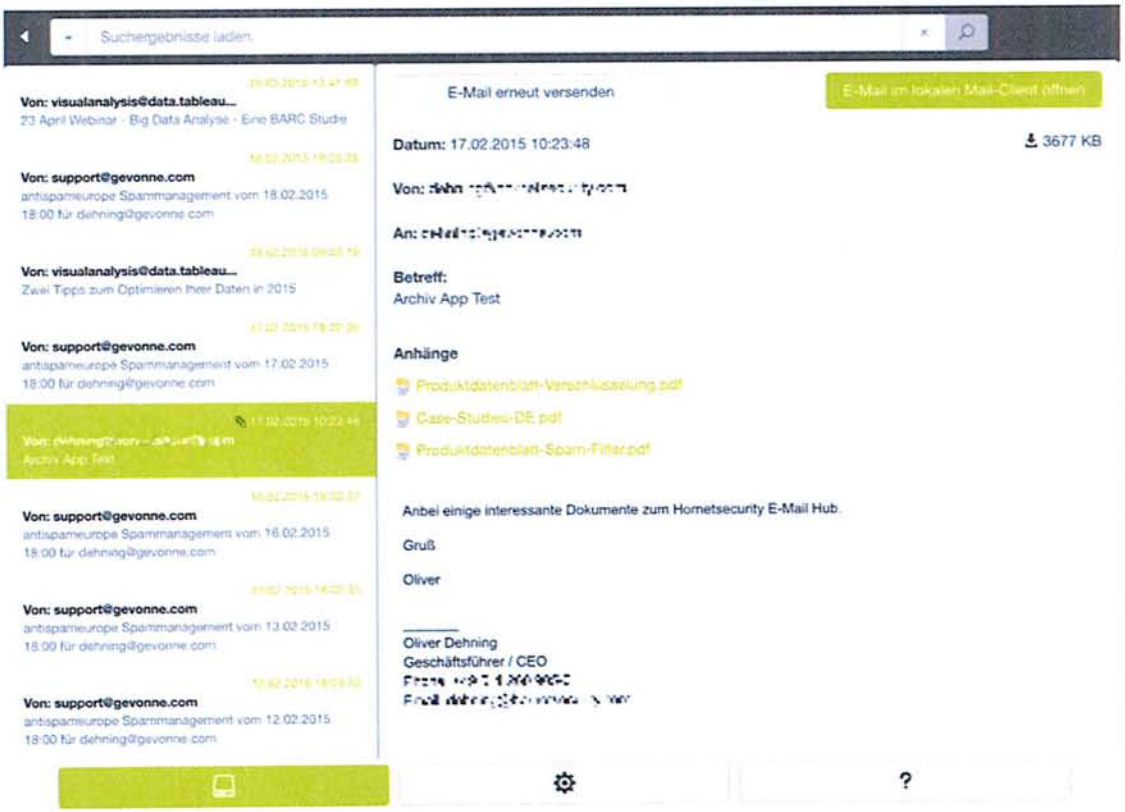


HK2 Rechtsanwälte

- Hornetsecurity Outlook Plugin



- Aeternum Mobile App



IV. GETROFFENE MAßNAHMEN

Folgende technischen und organisatorischen Maßnahmen sind von Hornetsecurity, neben den Maßnahmen aus der technischen Beschreibung (Ziffer III), vorgesehen:

1. Zutrittskontrolle

- Kontrolle der Identität per amtlichem Ausweis; wird durchgeführt durch das Personal des jeweiligen Rechenzentrums im Kontrollraum vor dem Zutritt in das Rechenzentrum.
- Überwachung der Rechenzentrum-Räume erfolgt per Videosystem (Tageslicht- und Infrarotkameras).
- Zugang zum Rechenzentrum erfolgt über zwei Zugangskontrollen:
    - Tür-Gegensprechanlage zum Kontrollraum mit elektrischen Türöffnern,
    - Tür-Schließsystem mit Magnetkarte.
- Zusätzlich sind die Racktower von Hornetsecurity mit eigenem Schließsystem versehen.
- Der Zugang wird mit Vermerk von Zugangszeitpunkt, Name und Firma, sowie mit Zugangsende protokolliert.

2. Zugangskontrolle

- Kennwort-Policy: mind. 8 Zeichen, mind. 3 von 4 Kriterien (Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen), Wechselintervall: 6 Monate.
- Pro Mitarbeiter besteht ein Benutzerstammsatz.
- Benutzerrechte sind auf Tätigkeitsbereiche eingeschränkt.
- Sämtliche Systeme werden durch geeignete Firewallsysteme vor unerlaubten Zugriffen geschützt, Zugänge bei Systemen sind auf eng definierte IP-Adressbereiche beschränkt.
- Das Archiv wird umfangreich verschlüsselt, sofern E-Mails nicht schon durch den Kunden verschlüsselt wurden:
    - Festplattenverschlüsselung: Diese wirkt als Schutz gegen Zugriffe, wenn Festplatten planmäßig oder durch deliktische Handlungen ausgebaut werden.

- E-Mail-Verschlüsselung: Daten werden vor der Speicherung im Archiv verschlüsselt. Header und Body der E-Mail werden getrennt per AES-256 verschlüsselt. Jedem Kunden wird ein zufälliger 16-stelliger alphanumerischer Schlüssel zugewiesen. Dieser Schlüssel wird in einer Schlüsseltabelle gespeichert. Die Schlüsseltabelle ist auf einem von den Archivdaten physisch getrennten System mit getrennten Zugängen abgelegt. Die Schlüsseltabelle wird redundant repliziert und täglich durch Backup gesichert.

3. Zugriffskontrolle

- Zugangsberechtigungen nur für Bereiche, die für spezifische Tätigkeiten benötigt werden (rollenbasierte Berechtigung).
- Kontrollen bzgl. unberechtigter Zugangsversuche (IDS/ IPS).
- Transaktionsprotokollierung jeglicher Systemänderungen.
- 4-Augenprinzippflicht für Software-Änderungen.

4. Weitergabekontrolle

- Externe Zugriffe auf Daten erfolgen ausschließlich über VPN.
- Offline-Arbeitsdateien (Notebooks etc.) liegen ausschließlich auf verschlüsselten Datenträgern vor.

5. Eingabekontrolle

- Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege wird gewährleistet.
- Jegliche Datenveränderung wird transaktionsorientiert protokolliert.
- Ein Verändern des Protokolls ist nicht möglich. Dadurch kann jederzeit auch nachträglich festgestellt werden, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

6. Auftragskontrolle

- Die Verarbeitung von Kundendaten wird von Hornetsecurity selbst durchgeführt und nicht an Dritte vergeben.
- Bei der Leistungserbringung werden lediglich Rechenzentrumsbetreiber mit folgenden Leistungen betreut: Physische Gebäudesicherung, Betrieb der Löschanlage, unterbrechungsfreie Stromversorgung, Klimatisierung, Internetanbindung, Bereitstellung von Racks, teilweisen Ein- und Ausbau von Systemen, teilweise Durchführung eines Neustarts über Reset- oder Power-

Button, Betrieb des lokalen RZ-Netzwerks zur Ankoppelung der Netzwerk-Segmente, inklusive Router- oder Switche-Betrieb.

- Sämtliche von Hornetsecurity genutzten, datenverarbeitenden Systeme - außerhalb von Netzwerkkomponenten wie Routern und Switches - sind in Besitz von Hornetsecurity und werden von Hornetsecurity durch eigenes Personal aufgebaut und betrieben. Netzwerkverbindungen sind grundsätzlich verschlüsselt. Die Rechenzentrumsbetreiber haben keinen Einblick in Kundendaten.

7. Verfügbarkeitskontrolle

- Hornetsecurity setzt bei der Datenverarbeitung mindestens zwei unabhängige und räumlich getrennte Rechenzentren ein. Jedes dieser Rechenzentren verfügt über:
    - redundante Stromversorgung,
    - redundante Netzwerkversorgung,
        - redundante Klimatisierung,
        - redundante Löschanlagen.
- Die Datenverarbeitung wird vollständig mit dem Betrieb eines einzelnen RZ gewährleistet. Das zweite und weitere RZ werden zur Erhöhung der Redundanz eingesetzt.
- Daten werden grundsätzlich auf gespiegelten Datenträgern durch geeignete RAID-Verfahren gespeichert.
- Zentrale Datensysteme sind zusätzlich gedoppelt mit automatischer Replikation sowie Hot-Fail-Over-Funktionalitäten ausgestattet.
- Daten werden zusätzlich regelmäßig gesichert, um ältere Datenstände wiederherstellen zu können.

8. Trennungsgebot

- Alle Daten werden nach Mandanten getrennt in dedizierten Datenbanken gespeichert.
- Für interne Zwecke (z. B. Entwicklung, Test und Backup) werden getrennte Systeme mit eigener Datenstruktur genutzt.

HK2 Rechtsanwälte

V. RECHTLICHE WÜRDIGUNG

1. Voraussetzungen - GoBD

Die GoBD regeln die Aufbewahrung von handelsrechtlich und steuerrechtlich relevanten Daten und Dokumenten in elektronischer Form. Die GoBD wurden durch Schreiben des Bundesfinanzministeriums am 14. November 2014 (GZ: V A 4 - S 0316/13/10003, DOK: 2014/0353090) in elektronischer Form publiziert.

Online abrufbar unter:

http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=2).

Die GoBD sind ab 1. Januar 2015 gültig. Sie lösen die Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) und die Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) ab.

Die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen ist nach den gleichen Prinzipien zu beurteilen wie die Ordnungsmäßigkeit bei manuell erstellten Büchern oder Aufzeichnungen.

Die GoBD stellt fest, dass technische Vorgaben und Standards insbesondere angesichts des schnellen technischen Fortschritts nicht festgeschrieben werden können, auch angesichts der sehr großen Unterschiede im organisatorischen Umfeld der verschiedenen Unternehmen. Es wird daher durchaus Fallkonstellationen geben, wo nicht allein aus den Ausführungen der GoBD entschieden werden kann, ob ein bestimmter Sachverhalt den Ordnungsmäßigkeitskriterien entspricht oder nicht. In solchen Situationen ist dann laut GoBD über einen Analogieschluss festzustellen, ob die Ordnungsvorschriften eingehalten wurden. So kann z. B. beurteilt werden, ob ein elektronischer Zugriffsschutz die gleiche Sicherheit bietet wie die Aufbewahrung von Papierdokumenten in einem verschlossenen Schrank.

Eine E-Mail, die allein zu Transportzwecken dient, wird mit einem bloßen Briefumschlag verglichen, der daher nicht aufbewahrungspflichtig sein kann. Sofern eine E-Mail aber funktional nicht nur zum Transport z. B. einer elektronischen Rechnung genutzt wird, sondern einen eigenständigen Handels- und Geschäftsbrief darstellt, ist der Fall gegensätzlich zu beurteilen (Rdn. 121 GoBD). Die nachfolgende Prüfung wird durchgehend vom letzten Fall ausgehen.

HK2 Rechtsanwälte

1.1. Ziffer 3 GoBD – Allgemeine Anforderungen

1.1.1. Gesetzlicher Rahmen

Die Anforderungen an die Ordnungsmäßigkeit ergeben sich aus:

- außersteuerlichen Rechtsnormen (z. B. den handelsrechtlichen Grundsätzen einer ordnungsgemäßen Buchführung gem. §§ 238, 239, 257, 261 HGB), die gem. § 140 Abgabenordnung (AO) für das Steuerrecht nutzbar gemacht werden können, wenn sie für die Besteuerung von Bedeutung sind und
- steuerlichen Ordnungsvorschriften (insbesondere gem. §§ 145 bis 147 AO).

Die allgemeinen Ordnungsvorschriften in den §§ 145 bis 147 AO gelten nicht nur für Buchführungs- und Aufzeichnungspflichten nach § 140 AO und nach den §§ 141 bis 144 AO. Insbesondere § 145 Abs. 2 AO betrifft alle zu Besteuerungszwecken gesetzlich geforderten Aufzeichnungen, also auch solche, zu denen der Steuerpflichtige aufgrund anderer Steuergesetze verpflichtet ist, wie z. B. nach § 4 Abs. 3 Satz 5, Abs. 7 Einkommensteuergesetz (EStG) und nach § 22 Umsatzsteuergesetz (UStG) (BFH-Urteil vom 24. Juni 2009, BStBl II 2010 S. 452).

1.1.2. Anforderungen nach den GoBD

Bei der Führung von Büchern und sonst erforderlichen Aufzeichnungen in elektronischer oder in Papierform sind die folgenden Anforderungen zu beachten (Rdn. 26 ff.):

- Grundsatz der Nachvollziehbarkeit und Nachprüfbarkeit (siehe unter 1.1.3),
- Grundsätze der Wahrheit, Klarheit und fortlaufenden Aufzeichnung (siehe unter 1.1.4):
  - Vollständigkeit (siehe unter 1.1.4.1),
  - Richtigkeit (siehe unter 1.1.4.2),
  - zeitgerechte Buchungen und Aufzeichnungen (siehe unter 1.1.4.3),
  - Ordnung (siehe unter 1.1.4.4),
  - Unveränderbarkeit (siehe unter 1.1.4.5).

Diese Grundsätze müssen während der Dauer der Aufbewahrungsfrist nachweisbar erfüllt werden und erhalten bleiben.

Nach § 146 Abs. 6 AO gelten die Ordnungsvorschriften auch dann, wenn der Unternehmer elektronische Bücher und Aufzeichnungen führt, die für die Besteuerung von Bedeutung sind, ohne hierzu verpflichtet zu sein.

Der Grundsatz der Wirtschaftlichkeit rechtfertigt es nicht, dass Grundprinzipien der Ordnungsmäßigkeit verletzt und die Zwecke der Buchführung erheblich gefährdet werden. Die zur Vermeidung einer solchen Gefährdung erforderlichen Kosten muss der Steuerpflichtige genauso in Kauf nehmen wie alle anderen Aufwendungen, die die Art seines Betriebes mit sich bringt (BFH Urt. v. 26.03.1968, BStBl II S. 527).

1.1.3. Nachvollziehbarkeit und Nachprüfbarkeit (§ 145 Abs. 1 AO, § 238 Abs. 1 Satz 2 und Satz 3 HGB)

Die Verarbeitung der einzelnen Geschäftsvorfälle sowie das dabei angewandte Buchführungs- oder Aufzeichnungsverfahren müssen nachvollziehbar und nachprüfbar sein.

Aeternum ist in der technischen Beschreibung umfassend dargestellt. Das Aufzeichnungsverfahren ist daher für den Kunden nachvollziehbar. Hornetsecurity ist der E-Mail-Kommunikation des Kunden systemisch vorgeschaltet und erfasst daher lückenlos alle aus- und eingehenden E-Mails.

Das Verfahren führt zu einer nachvollziehbaren Verarbeitung des Geschäftsvorfalls. Einem sachverständigen Dritten wird es ermöglicht, Geschäftsvorfälle in der Entstehung und Abwicklung lückenlos zu verfolgen. Es ist insbesondere nicht dem einzelnen Mitarbeiter in einem Unternehmen überlassen, ob und inwiefern eine E-Mail archiviert wird oder nicht.

1.1.4. Wahrheit, Klarheit, fortlaufende Aufzeichnung

1.1.4.1. Vollständigkeit (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB)

Die Geschäftsvorfälle sind vollzählig und lückenlos aufzuzeichnen (Grundsatz der Einzelaufzeichnungspflicht). Alle E-Mails werden exakt so im Archiv gespeichert, wie sie die Gateways bzw. Relays von Hornetsecurity erreichen.

Externe E-Mails sind dabei solche E-Mails, die nicht direkt den Domains zuzuordnen sind, die vom Mailserver des Kunden selbst bedient werden. Externe E-Mails erreichen den Kunden grundsätzlich von außen durch das Internet per SMTP bzw. werden per SMTP zu einem anderen Mailserver übertragen (externes Routing). Hierbei wird gleichzeitig eine vollständige Kopie im E-Mail-Archiv bei Hornetsecurity gespeichert. Dadurch ist sichergestellt, dass eingehende E-Mails vom Empfänger nicht vor der Speicherung im Archiv manipuliert werden können.

Ausgehende E-Mails werden vom Mailserver des Kunden an die Mail-Relays von Hornetsecurity geleitet und erst von dort dem Empfänger zugestellt. Eine Kopie der ausgehenden E-Mail wird vom Mail-Relay im E-Mail-Archiv gespeichert. Auch hier ist sichergestellt, dass die E-Mail exakt so, wie sie dem Empfänger zugeschickt wurde, im Archiv gespeichert wird. Eine zwischenzeitliche Manipulation durch den Absender ist ausgeschlossen.

Es liegt auch keine unzulässige Mehrfachaufzeichnung vor, da Aeternum ein technisch und organisatorisch getrenntes System darstellt und mehrfache Auswirkungen ausgeschlossen sind.

1.1.4.2. Richtigkeit (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB)

Eine Manipulation der E-Mails ist beim Versand oder im Archiv ist ausgeschlossen (siehe 1.1.4.1 und 1.1.4.5).

1.1.4.3. Zeitgerechte Aufzeichnungen

E-Mails werden von Aeternum unmittelbar an den jeweiligen Empfänger weitergeleitet. Eine E-Mail-Archivierung erfolgt ebenso unmittelbar.

1.1.4.4. Ordnung (§ 146 Abs. 1 AO, § 239 Abs. 2 HGB)

Die geschäftlichen Unterlagen dürfen nicht planlos gesammelt und aufbewahrt werden. Ansonsten würde dies mit zunehmender Zahl und Verschiedenartigkeit der Geschäftsvorfälle zur Unübersichtlichkeit führen und die Gefahr erhöhen, dass Unterlagen verloren gehen oder später leicht entfernt werden können.

Die Speicherung der archivierten E-Mails erfolgt in Datenbanken. Gespeichert werden Header-Informationen (Absender, Empfänger, Betreff, Datum) sowie ein Volltextindex in einer No-SQL Datenbank und die komplette E-Mail („so wie sie ist") kundenbasiert in einer SQL Datenbank.

1.1.4.5. Unveränderbarkeit (§ 146 Abs. 4 AO, § 239 Abs. 3 HGB)

Eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.

Alle E-Mails werden exakt so im Archiv gespeichert, wie sie die Gateways bzw. Relays von Hornetsecurity erreichen. Eine Manipulation ist selbst durch Mitarbeiter des Kunden nicht möglich.

Die Veränderung von einmal im Archiv gespeicherten Daten durch den Kunden ist technisch ausgeschlossen. Einmal im Archiv gespeicherte Daten können daher erst nach Ablauf der eingestellten Archivierungsfrist gelöscht werden. Nach Ablauf der Archivierungsfrist erfolgt die Löschung der Archivdaten automatisch.

1.2. Ziffer 7 GoBD – Datensicherheit

Das eingesetzte Datenverarbeitungs-System (DV-System) muss gegen Verlust (z. B. Unauffindbarkeit, Vernichtung, Untergang und Diebstahl) und gegen unberechtigte Eingaben und Veränderungen (z. B. durch Zugangs- und Zugriffskontrollen) geschützt werden. Werden die Daten nicht ausreichend geschützt und können deswegen nicht mehr vorgelegt werden, so ist die Buchführung formell nicht mehr ordnungsmäßig.

Das E-Mail-Archiv Aeternum wird als Cloud-Lösungen angeboten. Bereitstellung, Betrieb und Überwachung der Systeme und Services erfolgen durch Hornetsecurity. Die Lösungen werden über mehrere gesicherte deutsche Rechenzentren erbracht, sofern nicht auf Wunsch des Kunden ausdrücklich etwas anderes vereinbart wird. Hornetsecurity speichert Daten ausschließlich in Deutschland. Standorte der Rechenzentren sind: Hannover, Düsseldorf, Frankfurt und München.

Die genutzten Rechenzentren verfügen über mehrfache Absicherung durch Unterbrechungsfreie Stromversorgung (USV), Dieselaggregate sowie mehrfache Netzanbindung mit doppelt ausgelegten Netz-Komponenten (Router etc.). Die von Hornetsecurity in den Rechenzentren betriebenen Systeme sind untereinander redundant, d. h. bei Ausfall eines einzelnen Systems wird die Leistung durch andere Systeme übernommen. Weder der Ausfall einzelner Systeme, noch der eines kompletten Rechenzentrums führen zur Unterbrechung des Mail-Verkehrs.

Eine umfassende Darstellung der erforderlichen Datensicherheitsmaßnahmen hinsichtlich Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle finden sich unter Ziffer 2. Es wird umfassend auf dortige Ausführungen verwiesen.

1.3. Ziffer 9 GoBD – Aufbewahrung

Der sachliche Umfang der Aufbewahrungspflicht in § 147 Abs. 1 AO besteht grundsätzlich nur im Umfang der Aufzeichnungspflicht.

1.3.1. Ordnung

Hierzu Rdn. 117 GoBD:

> *„Die aufbewahrungspflichtigen Unterlagen müssen **geordnet** aufbewahrt werden. Ein bestimmtes Ordnungssystem ist nicht vorgeschrieben. Die Ablage kann z. B. nach Zeitfolge, Sachgruppen, Kontenklassen, Belegnummern oder alphabetisch erfolgen. Bei elektronischen Unterlagen ist ihr Eingang, ihre Archivierung und ggf. Konvertierung sowie die weitere Verarbeitung zu protokollieren. Es muss jedoch sichergestellt sein, dass ein sachverständiger Dritter innerhalb angemessener Zeit prüfen kann." (Hervorhebung durch Verfasser)*

Die Speicherung der archivierten E-Mails erfolgt in Datenbanken. Gespeichert werden Header-Informationen (Absender, Empfänger, Betreff, Datum) sowie ein Volltextindex in einer No-SQL Datenbank und die komplette E-Mail („so wie sie ist") kundenbasiert in einer SQL Datenbank.

1.3.2. Formgleichheit

Die Aufbewahrung hat nach Rdn. 119 GoBD zudem in der **Form** zu erfolgen, in der sie im Unternehmen entstanden ist. Es ist daher nicht ausreichend, den E-Mail-Verkehr auszudrucken und in Papierform zu speichern. Per E-Mail eingehende Rechnungen im PDF-Format müssen damit als elektronische Unterlagen für die Dauer der Aufbewahrungsfrist geführt werden. Durch das E-Mail-Archiv von Hornetsecurity wird diese Anforderung erfüllt. Alle E-Mails werden exakt so im Archiv gespeichert, wie sie die Gateways bzw. Relays von Hornetsecurity erreichen. Der Kunde hat insbesondere nicht mehr die Abwägung zu treffen, ob und inwiefern eine Speicherung ausschließlich in Papierform vielleicht doch zulässig sein könnte (z. B. Rechnung wird auch in Papierform versandt), da ausnahmslos eine Speicherung des E-Mail-Verkehrs erfolgt und unzulässige Medienbrüche ausgeschlossen werden können.

Mit dem E-Mail-Archiv von Hornetsecurity werden zudem Fehler bei der Bestimmung von Aufbewahrungspflichten vermieden. Bezüglich der Speicherung des E-Mail-Verkehrs nehmen die GoBD folgende Differenzierung vor:

> *„Bei den Daten und Dokumenten ist - wie bei den Informationen in Papierbelegen - auf deren Inhalt und auf deren Funktion abzustellen, nicht auf deren Bezeichnung. So sind beispielsweise **E-Mails** mit der Funktion eines **Handels- oder Geschäftsbriefs** oder eines Buchungsbelegs in elektronischer Form aufbewahrungspflichtig. Dient eine E-Mail nur als „**Transportmittel**", z. B. für eine angehängte elektronische Rechnung, und enthält darüber hinaus keine weitergehenden aufbewahrungspflichtigen Informationen, so ist diese nicht aufbewahrungspflichtig (wie der bisherige Papierbriefumschlag)."*

Diese Differenzierung ist für den einzelnen Mitarbeiter im Einzelfall nicht leicht zu treffen. Fehlentscheidungen sind beim E-Mail-Archiv von Hornetsecurity dahingehend ausgeschlossen, da automatisch der gesamte E-Mail-Verkehr archiviert wird.

1.3.3. Index und Auswertbarkeit

Ein elektronisches Dokument ist mit einem nachvollziehbaren und eindeutigen **Index** zu versehen. Der Erhalt der Verknüpfung zwischen Index und elektronischem Dokument muss während der gesamten Aufbewahrungsfrist gewährleistet sein. Es ist sicherzustellen, dass das elektronische Dokument unter dem zugeteilten Index verwaltet werden kann. Die Dokumente müssen zudem entsprechend auch **maschinell auswertbar** (§ 147 Abs. 2 Nr. 2 AO) sein.

Die Speicherung der archivierten E-Mails erfolgt in Datenbanken. Gespeichert werden Header-Informationen (Absender, Empfänger, Betreff, Datum) sowie ein Volltextindex in einer No-SQL Datenbank und die komplette E-Mail „so wie sie ist" kundenbasiert in einer SQL Datenbank. Aeternum kann E-Mails nicht nur anhand indizierter Parameter (Zeit, Datum, Absender, Empfänger, Betreff) darstellen, sondern ermöglicht dem Kunden eine umfassende Volltextsuche, die auch den E-Mail-Text erfasst. Formatumwandlungen (z. B. in PDF), die ein Hindernis bei der Auswertbarkeit der E-Mail begründen könnten, finden in Aeternum nicht statt. E-Mail-Anhänge werden ebenfalls in dem Format gespeichert, in dem diese versandt oder empfangen wurden. Eine Verwaltung und Auswertung der Dokumente ist anhand dieser Daten für E-Mails unproblematisch möglich.

In quantitativer und qualitativer Hinsicht wird Aeternum die gleichen Auswertungen der aufzeichnungs- und aufbewahrungspflichtigen Daten ermöglichen, als wären diese noch im Produktivsystem vorhanden. Auf in Aeternum gespeicherte Daten können autorisierte Benutzer über verschiedene Interfaces zugreifen:

- Hornetsecurity Control Panel,
- Hornetsecurity Outlook Plugin,
- Aeternum Mobile App.

Outlook-Plugin und Mobile App ermöglichen den direkten Abruf archivierter E-Mails sowie deren Anhänge und darauf folgend Bearbeitung und Weiterleitung der Daten. Zusätzlich können archivierte E-Mails aus dem Archiv erneut in die Mailbox des Benutzers zugestellt werden. Im Control Panel kann nur eine Textversion der E-Mail eingesehen und die E-Mail erneut ausgelöst werden.

Für ein Archivsystem liegen die Daten daher ohne wesentliche Nutzungseinschränkungen vor und können ähnlich wie im Produktivsystem genutzt werden.

Probleme in der Auswertbarkeit könnten sich aus der eingesetzten **Verschlüsslungstechnik** ergeben. Aeternum verschlüsselt die E-Mail-Archivdaten automatisch mittels eines kundenspezifischen, 16-stelligen, alphanumerischen Schlüssels. Hierbei ist sicherzustellen, dass die verschlüsselten Unterlagen im DV-System in entschlüsselter Form zur Verfügung stehen. Werden Signaturprüfschlüssel verwendet, sind die eingesetzten Schlüssel aufzubewahren.

Der Schlüssel wird von Hornetsecurity in einer Schlüsseltabelle gespeichert. Die Schlüsseltabelle ist auf einem von den Archivdaten physisch getrennten System mit getrennten Zugängen abgelegt. Die Schlüsseltabelle wird redundant repliziert und täglich durch Backup gesichert. Bei Zugriff des Kunden auf das Archiv, liegen die Daten automatisch entschlüsselt vor. Es werden daher hinreichende Maßnahmen getroffen, die Lesbarkeit der Daten sicherzustellen.

Hinsichtlich der **Auslagerung von Daten aus dem Produktivsystem und Systemwechsel bzw. einer Daten-Migration** ergeben sich keine besonderen Anforderungen, da bisher beim Kunden bestehende Archivbestände bei diesem verbleiben und nicht in Aeternum überführt werden. Datenbestände, Hard- und Software müssen dahingehend vom Kunden weiter betrieben werden, solange hinsichtlich der nicht in Aeternum gespeicherten Daten Aufbewahrungspflichten bestehen.

2. IT-Sicherheitsmaßnahmen nach § 9 BDSG

2.1. Voraussetzungen

Welche konkreten, gesetzlichen Anforderungen an die IT-Sicherheit eines Onlineportals gestellt werden, ist für personenbezogene Daten in § 9 BDSG ausdrücklich geregelt:

> *„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

Die Vorschrift erfährt eine Konkretisierung durch die Anlage zu § 9 S. 1 BDSG. Demnach sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

- *Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren* ***(Zutrittskontrolle)****,*
- *zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können* ***(Zugangskontrolle)****,*
- *zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der*

Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können ***(Zugriffskontrolle)****,*

- *zu gewährleisten, 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)****,*
- *zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind* ***(Eingabekontrolle)****,*
- *zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können* ***(Auftragskontrolle)****,*
- *zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind* ***(Verfügbarkeitskontrolle)****,*
- *zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

Grundziel aller Maßnahmen bildet die Gewährleistung bestimmter Sicherheitsstandards, die die

- **Verfügbarkeit,**
- **Unversehrtheit und**
- **Vertraulichkeit**

sicherstellen (§ 2 Abs. 2 BSIG).

Der Begriff der technischen und organisatorischen Maßnahmen ist daher weit auszulegen. Es können unterschiedliche Maßnahmen hierunter verstanden werden, die gesetzmäßige Datenschutzkontrollen und einen ordnungsgemäßen Betriebsablauf gewährleisten.

Dies führt nicht dazu, dass schrankenlos Maßnahmen ergriffen werden müssen, um die genannten Sicherheitsziele zu verwirklichen. Das Schutzziel steht nach § 9 S. 2 BDSG ausdrücklich unter einem **Verhältnismäßigkeitsvorbehalt**:

> *„Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

Primär ist daher die Schutzbedürftigkeit der zu verarbeitenden Daten mit dem Aufwand der Sicherungsmaßnahmen im konkreten Einzelfall ins Verhältnis zu setzen.

Je nach der **Art der zu schützenden Datenkategorien und Zweck der Datenverarbeitung** ist das Schutzniveau der technischen und organisatorischen Maßnahmen anzupassen. Die Planung und Vorbereitung von Datensicherungsmaßnahmen erfolgt daher zweckmäßigerweise auf der Grundlage einer vorhergehenden Risikoanalyse (Gola/ Schomerus, BDSG § 9 Rdn. 9).

Eine Risikoanalyse hat folgende Parameter abwägend zu berücksichtigen:

- Art der Daten/ Informationen,
- Schadensrisiko,
- Zweck der Datenverarbeitung,
- objektive Risikolage (allgemein und branchenspezifisch),
- subjektive Risikolage,
    - Bereichsspezifische Vorgaben (z. B. Sozial- und Berufsrecht),
    - zurückliegende Vorfälle,
    - vertragliche Pflichten.
- Unternehmensgröße/ wirtschaftliche Leistungsfähigkeit,
- eigene Sachkunde.

Die aufgezeigten Parameter verdeutlichen, dass eine pauschale Beurteilung nur bedingt möglich ist. Bei der Abwägung müssen auch individuelle Parameter des Kunden einfließen (subjektive Risikolage, Unternehmensgröße, Art der Daten). Das Gutachten kann daher nur grundsätzliche Aussagen dazu treffen, ob es Kunden regelmäßig möglich ist, unter Anreicherung einer eigenen Risikoanalyse, den gegenständlichen Dienst zu nutzen.

2.2. Risikoanalyse

Zweck der Risikoanalyse ist es, zu ermitteln, welcher Schutz für die verarbeiteten Daten ausreichend und angemessen ist.

Maßgeblich sind hierzu u. a. die Art bzw. Sensibilität der verarbeiteten Daten und der zu erwartenden Schäden, die bei einer Beeinträchtigung der genannten Schutzziele **Verfügbarkeit, Unversehrtheit und Vertraulichkeit** entstehen können.

Hierbei sind drei Schutzbedarfskategorien anerkannt:

- „normal": Die Schadensauswirkungen sind in der Regel begrenzt und überschaubar. Ein solcher Schaden indiziert im Regelfall keine nennenswerten Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen.
- „hoch": Die Schadensauswirkungen sind in der Regel beträchtlich. Ein solcher Schaden führt im Regelfall zu beträchtlichen Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen.
- „sehr hoch": Ein solcher Schaden kann zu existenziell bedrohlichen oder sogar katastrophalen Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen führen.

2.2.1. Datenkategorien und Schadensrisiko

2.2.1.1. Bezüglich E-Mail-Inhalt – Vertraulichkeit und Unversehrtheit

Die Art der verarbeiteten Daten und das damit einhergehende Schadensrisiko unterscheidet sich stark je nach Nutzungsumfang des Portals bzw. den Einsatz von E-Mails in der Unternehmenskommunikation. Eine genaue Festlegung der Datenkategorien ist kaum möglich. Inhalte einer E-Mail-Kommunikation können belanglos (z. B. Übersendung von Werbematerial) oder extrem relevant sein (z. B. Vertragsunterlagen eines Großprojekts). Im Ergebnis kann daher nicht ausgeschlossen werden, dass E-Mails über Aeternum archiviert werden, bei deren Abhandenkommen für ein Unternehmen beträchtliche Konsequenzen drohen. Dies gilt umso mehr, da es derzeit bei der Nutzung von E-Mails oft noch an der erforderlichen Sensibilität des betreffenden Mitarbeiters oder der Unternehmensleitung selbst fehlt, entsprechende Einschränkungen bei der Nutzung vorzunehmen bzw. anzuweisen.

Es ist daher eine Schutzkategorie „hoch" gegeben.

Von einer Schadenskategorie „sehr hoch" (existenziell bedrohlichen oder sogar katastrophalen Konsequenzen) ist hingegen nicht auszugehen. Sofern E-Mails solche Inhalte zum Gegenstand haben, wäre die (unverschlüsselte) E-Mail als Kommunikationsmittel jedenfalls ungeeignet. Unverschlüsselte E-Mails können mit Postkarten verglichen werden, die von Dritten leicht mitgelesen und manipuliert werden können. Es liegt daher klar in der Verantwortung des Kunden, solche E-Mails nicht unverschlüsselt zu versenden, die unter die Schadenskategorie „sehr hoch" fallen. Jedenfalls kann in diesem Fall die Anforderung an die IT-Sicherheit des Archivierungssystems nicht bedeutend höher liegen, als an den Versand selbst.

Sofern daher vom Kunden Inhalte mit der Schadenskategorie „sehr hoch" versendet werden, ist davon auszugehen, dass dies durch den Kunden selbst verschlüsselt zu

erfolgen hat. Aeternum unterliegt in diesem Punkt auch keinen technischen Einschränkungen. Das System speichert auch durch den Kunden verschlüsselte E-Mails ohne Einschränkungen. Die E-Mail kann in diesem Fall vom Kunden weiterhin anhand folgender Parameter im Archiv ermittelt werden: Absender, Empfänger, Zeitpunkt des Versandes und Header.

Die Schadenskategorie „hoch" dürfte daher dem vorhersehbaren Nutzungsumfang der Kunden entsprechen. Für eine weitergehende Nutzung sind primär Maßnahmen durch den Kunden zu ergreifen, die nicht im Herrschaftsbereich von Hornetsecurity liegen (z. B. Verschlüsslung, Wahl alternativer Kommunikationsmittel, einzelfallbezogene Maßnahmen).

2.2.1.2. Bezüglich Verfügbarkeit des gesamten Systems

Sofern IT-Sicherheitsmaßnahmen die Verfügbarkeit von Aeternum sicherzustellen haben (Datenverlust und Blockade), ist von einem „sehr hohen" Schadensrisiko auszugehen, jedenfalls hat der Kunde in diesem Zusammenhang keine Möglichkeiten andere, Sicherheitsmaßnahmen zu treffen. Den bestehenden Leistungsumfang zu Aeternum zugrundgelegt, muss sich der Kunde hierzu auch nicht veranlasst sehen.

Ein gesteigertes Schadenspotential liegt hierbei nicht in der Brisanz des einzelnen E-Mail-Inhalts, sondern der Datenmenge selbst. Aeternum archiviert die gesamte E-Mail-Korrespondenz eines Unternehmens. Störungen und Verlust würden ein entsprechendes Ausmaß annehmen. Dies geht, wie oben ausgeführt, mit einer stetig wachsenden Bedeutung der E-Mail als Kommunikationsmittel einher. Nicht zuletzt aufgrund der niedrigen Kosten und schnellen Zustellung ist die E-Mail oft das Kommunikationsmittel der ersten Wahl.

Gegen ein „sehr hohes" Schadensrisiko kann nur angeführt werden, dass die Daten in diesem Fall nur im Archiv nicht mehr zur Verfügung stehen, aber im Produktivsystem noch uneingeschränkt vorhanden sind.

Im Zweifelsfall ist hinsichtlich der Verfügbarkeit von der höheren Schutzkategorie auszugehen.

2.2.2. Zweck der Datenverarbeitung

Aus dem Datenverarbeitungszweck ergeben sich keine erhöhten Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen. Hornetsecurity verarbeitet die Daten nicht selbst und hat kein eigenes Interesse an den Daten. Vielmehr dient die Plattform nur der E-Mail-Archivierung für Dritte.

2.2.3. Sachkunde und Risikolage

Als professioneller Dienstleister für Cloud-basierte E-Mail-Archivierungssysteme, muss Hornetsecurity ein hohes IT-Sicherheitsniveau einhalten. Kunden dürfen es bei entsprechend spezialisierten Dienstleistern erwarten, dass diese nicht nur ein Mindestniveau einhalten, sondern auch Maßnahmen ergreifen, die einer erhöhten Bedrohungslage Rechnung tragen. Da es sich bei Aeternum aber nicht um eine anwender- oder branchenspezifische Lösung handelt und pauschal die gesamte Kommunikation erfasst werden soll, wird das IT-Sicherheitsniveau im Allgemeinen mit „hoch" zu bemessen sein.

Aus der Risikolage für Hornetsecurity selbst ergeben sich keine abweichenden Anforderungen an die zu treffenden technischen und organisatorischen Maßnahmen. Hornetsecurity hatte bisher keinen Datenverlust oder den Zugriff unbefugter Dritter auf die IT-Systeme zu verzeichnen.

2.3. Ergebnis

Die Schutzkategorie „hoch" hinsichtlich der Vertraulichkeit und Unversehrtheit vorausgesetzt, sind die getroffenen technischen und organisatorischen Maßnahmen als hinreichend zu betrachten. Es werden in allen von § 9 BDSG vorgesehenen Bereichen Sicherheitsmaßnahmen getroffen, die dem Schutzniveau der Daten gerecht werden.

Aeternum wird ausschließlich über zuverlässige und gesicherte Rechenzentren in Deutschland betrieben (Hannover, Düsseldorf, Frankfurt und München). Dort betreibt Hornetsecurity eigenverantwortlich gesondert gesicherte und mit eigenem Schließsystem versehene Racks. Daten werden somit bei der gesamten Verarbeitung nicht an Dritte weitergeben. Auf anderen Systemen werden Kundendaten nicht verarbeitet.

Neben den üblichen Zugangs- und Zugriffskontrollen (z. B. Kennwortrichtlinien, Vergabe von Benutzerrechten und Rollen, Zugriffsprotokollierung), wird der Zugang auf definierte IP-Adressbereiche beschränkt, alle Festplatten in Computersystemen werden grundsätzlich verschlüsselt und umfassend protokollierte Softwareänderungen können nur von zwei Personen gleichzeitig vorgenommen werden.

Eine Nutzung bzw. der Zugriff auf Aeternum ist ausschließlich über VPN möglich. Nutzungshandlungen werden nachvollziehbar dokumentiert, indem protokolliert wird, von wem Daten eingegeben, verändert oder entfernt wurden. Protokolle können folgend nicht manipuliert werden.

Bezüglich der Verfügbarkeit der Daten werden von Hornetsecurity demgegenüber „sehr hohe" Anforderungen erfüllt, so dass ein ungewollter Datenverlust praktisch ausgeschlossen werden kann. Hornetsecurity setzt mindestens zwei unabhängige und räumlich getrennte Rechenzenten ein (Hannover, Düsseldorf, Frankfurt und München). Hierbei kann eine vertragsgemäße Datenverarbeitung schon beim Betrieb eines Rechenzentrums gewährleistet werden. Das zweite Rechenzentrum dient nur der Ausfallsicherung (automatischer Replikation sowie Hot-Fail-Over-Funktionalitäten). Daten werden grundsätzlich auf gespiegelten Datenträgern durch geeignete RAID-Verfahren gespeichert. Es bestehen in jedem genutzten Rechenzentrum Redundanzen bezüglich aller gängigen Ausfallrisiken (Stromversorgung, Netzwerkversorgung, Klimatisierung, Löschanlagen). Darüber hinaus können ältere Datenbestände über regelmäßige Back-ups wieder hergestellt werden. Hornetsecurity verarbeitet zudem eigene Daten (z. B. Entwicklung und Test) in getrennten Systemen.

In Abwägung mit dem hohen und teilweise sehr hohen Schutzniveau der Daten sind die getroffenen technischen und organisatorischen Maßnahmen daher als auseichend zu werten.

Hinweis:
Das Gutachten hat ausschließlich die oben benannten Ziffern der GoBD und § 9 BDSG zum Gegenstand. Darüber hinaus bestehende rechtliche Anforderungen wurden nicht geprüft.

Es obliegt grundsätzlich dem Kunden von Aeternum, eine rechtliche Konformitätsprüfung der Nutzung und Datenübertragung, insbesondere im Verhältnis zu Dritten vorzunehmen (z. B. Arbeits-, Datenschutz- und Zivilrecht). Zudem bleibt es dem einzelnen Nutzer vorbehalten, das für die Datenverarbeitung erforderliche subjektive Schutzniveau anhand der oben beschriebenen technischen und organisatorischen Maßnahmen sowie der technischen Verfahrensbeschreibung selbst zu bestimmen und abzuwägen.

„Für die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen, einschließlich der eingesetzten Verfahren, ist allein der Steuerpflichtige verantwortlich. Dies gilt auch bei einer teilweisen oder vollständigen organisatorischen und technischen Auslagerung von Buchführungs- und Aufzeichnungsaufgaben auf Dritte" (Rdn. 21 GoBD).

Da die Plattform den E-Mail-Verkehr des gesamten Unternehmens betreffen kann, sind eine unüberschaubare ***Vielzahl von Fällen*** *denkbar, die weder umfassend antizipiert, noch dargestellt werden können. Bei der Bestimmung des Schutzniveaus sind zudem* ***bereichsspezifische Regelungen*** *für den jeweiligen Kunden zu berücksichtigen, die in diesem Gutachten nicht abgebildet werden können (z. B. Berufsrecht, Bankenrecht).*

Zudem hat das Unternehmen dafür Sorge zu tragen, dass die „Ordnungsmäßigkeit bei der Einrichtung und unternehmensspezifischen Anpassung des DV-Systems bzw. der DV-gestützten Verfahren im ***konkreten Unternehmensumfeld*** *und für die Dauer der Aufbewahrungsfrist erhalten bleibt" (Rdn. 23 GoBD, Hervorhebung durch Verfasser). Dies betrifft vor allem auch konkrete technische Vorgaben und Standards (z. B. zu Archivierungsmedien oder Kryptografieverfahren). Die GoBD sowie das BDSG treffen hierzu keine Festlegungen, da angesichts der rasch fortschreitenden Entwicklung und der ebenfalls notwendigen Betrachtung des organisatorischen Umfelds diese nicht festgelegt werden können (vgl. Rdn. 10 GoBD).*

Abschließend muss auch darauf hingewiesen werden, dass ***„Zertifikate" oder „Testate" Dritter*** *bei der Auswahl eines Softwareproduktes dem Unternehmen als Entscheidungskriterium dienen, diese jedoch gegenüber der Finanzbehörde keine Bindungswirkung entfalten (Rdn. 181 GoBD).*

Berlin, 05.08.2015

HK2 Rechtsanwälte
Hausvogteiplatz 11 A 10117 Berlin
Telefon +49 (0)30 27 89 00-0
Telefax +49 (0)30 27 89 00-10
www.hk2.eu mail@hk2.eu
Karsten U. Bartels LL.M.
Rechtsanwalt
Zertifizierter Datenschutzbeauftragter (TÜV)