Dienstbeschreibungen

DIE IN DEN ANHANG 2 UNTEN AUFGEFÜHRTEN DIENSTBESCHREIBUNGEN, DIE VOM KUNDEN NACH ABSCHNITT B DES VERTRAGS NICHT BESTELLT WURDEN, FINDEN NICHT AUF DEN KUNDEN ANWENDUNG.

Anhang 1
Allgemeines

1. Begriffsdefinitionen und Auslegung

1.1. In diesem Vertrag, einschließlich seiner Anlagen, haben die folgenden Begriffe, soweit nicht der Sachzusammenhang eindeutig entgegensteht, die nachfolgende Bedeutung:

"Massenmail"	meint ein Paket von mehr als fünftausend (5000) E-Mailnachrichten mit überwiegend gleichem Inhalt, die in einem einzelnen Vorgang oder in einer Reihe von entsprechenden Vorgängen versendet oder empfangen werden;
"E-Mail"	meint eine SMTP-Nachricht, die im Rahmen der Dienstleistung versendet oder empfangen wird;
"Gewöhnliche Geschäftszeiten"	meint Montag bis Freitag zwischen 08:30 und 17:30 (CET), ausschließlich der in Bayern geltenden Feiertage;
„nicht teilbares Dienst-Paket"	bedeutet ein Paket von Diensten gemäß Abschnitt B „Dienste und Gebühren", unter Vorbehalt von Punkt 3.7;
"Mitglied"	meint den Kunden und Organisationen, mit denen der Kunde durch Verwendung des Boundary-Encryption-Dienstes (Verschlüsselungsdienst) ein verschlüsseltes Netz betreibt;
„Offener Proxy"	bezeichnet einen Proxyserver, der so eingerichtet ist, dass unbekannten oder nicht autorisierten Dritten das Abrufen, Speichern oder Weiterleiten von DNS, Webseiten oder anderen Daten ermöglicht wird;
"Open Relay"	meint einen E-Mailserver, der so konfiguriert ist, E-Mails von nicht bekannten und nicht berechtigten Dritten zu empfangen und diese E-Mails an einen oder mehrere Empfänger weiterzuleiten, die nicht Nutzer des E-Mail-Systems sind, an das der Mailserver angebunden ist. Open Relay meint auch "Spam relay" und "public relay";
"Spam"	meint unerwünschte Werbe-E-Mails;
"Tower"	meint einen Cluster von lastverteilten E-Mailservern;
"Nutzer"	meint eine Person, eine Mailbox oder eine Maschine, die eine Dienstleistung nutzt;
"Virus"	meint (schädlichen) Programmcode, einschließlich eines sich selbst vervielfältigenden Bestandteils, der sich gewöhnlich (nicht notwendigerweise) als etwas anderes tarnt und/oder ungefragt überraschende und/oder schädliche Funktionen ausführen soll und meist dazu bestimmt ist, Computersysteme zu befallen.

2. Einleitung

2.1. Symantec ist ein Managed Services Provider, der auf dem Gebiet der internetbasierten E-Mail-, Instant-Message- und Web-Sicherheit spezialisiert ist.
2.2. Die Dienste werden vierundzwanzig (24) Stunden/Tag und sieben (7) Tage/Woche von dem Global Operations Center erbracht. Zum Umfang der Dienstleistungen gehören die Überprüfung von Hardware-Kapazität, von Service-Kapazitäten sowie die Auslastung von Netzwerk-Kapazitäten.
2.3. Die Dienste werden für Kunden erbracht, deren Email-Systeme fortlaufend über eine feste IP-Adresse an das Internet angebunden sind. Die Dienste stehen nicht für Kunden zur Verfügung, deren Email-Systeme durch einen telefonischen Verbindungsaufbau oder per ISDN-Leitungen angebunden sind oder deren IP-Adressen dynamisch vergeben werden.
2.4. Eingehende E-Mails, die von Symantec nicht an den Mail-Server eines Kunden geschickt werden können, werden von Symantec maximal sieben (7) Tage gespeichert.
2.5. Bei allen eingehenden E-Mails wird die IP-Kennung des Absenders überprüft. E-Mails aus einer Quelle mit schlechter Kennung (z. B. ein Spammer) werden verlangsamt, um die Auswirkung auf die Netzwerkkapazität zu minimieren.
2.6. Der Kunde sollte seine E-Mail-Server so konfigurieren, dass die maximale Anzahl von Empfängern pro ausgehender SMTP-Verbindung auf weniger als 500 Empfänger begrenzt wird. Ein Empfänger entspricht einer einzelnen E-Mail-Adresse. Eine E-Mail-Gruppe kann einen oder mehrere Empfänger enthalten. Falls eine eingehende oder ausgehende E-Mail mehr als 500 Empfänger in einer SMTP-Verbindung enthält, verarbeitet Symantec die ersten 500 Empfänger und sendet einen SMTP-Antwortcode an den sendenden E-Mail-Server mit der Anforderung, dass der Server die E-Mail erneut an die restlichen Empfänger versendet.

3. Management

3.1. "Geplante Wartung" meint Wartungsintervalle, die Symantec dem Kunden sieben (7) Tage vor Durchführung per E-Mail mitteilt und die zu einer Beeinträchtigung der Dienstleistungen mangels Verfügbarkeit des Tower Clusters führen können. Die Geplante Wartung wird acht (8) Stunden pro Kalendermonat nicht überschreiten und wird nie zwischen 8.00 Uhr und 18 Uhr Ortszeit durchgeführt.
3.2. Soweit möglich, werden geplante Wartungsarbeiten ohne Beeinträchtigung der Dienste erbracht. Dies wird grundsätzlich dadurch erreicht, dass die geplanten Wartungsarbeiten während Zeiten mit geringem Emailverkehrsvolumen durchgeführt werden sowie dadurch, dass die geplanten Wartungsarbeiten - soweit möglich - nur einzelne Teile des Netzwerks betreffen. Während der Durchführung der Wartungsarbeiten werden eingehende Emails an solche Teile des Netzwerks weitergeleitet, die nicht gewartet werden, um die Beeinträchtigung der Dienste gering zu halten.
3.3. Werden Notfallwartungen notwendig und ist wahrscheinlich, dass hierdurch die Dienste beeinträchtigt werden, wird sich Symantec bemühen, den betroffenen Kunden zu informieren und eine Alarm-Nachricht per ClientNet so schnell wie möglich, in jedem Fall innerhalb einer (1) Stunde nach dem Beginn der Notfallwartungsarbeiten zu versenden.

4. ClientNet

4.1. Ein integraler Bestandteil der Dienste ClientNet, ein internet-basiertes Konfigurations-, Management- und Reporting-Tool von Symantec. ClientNet wird dem Kunden über ein Passwort-geschütztes Login zur Verfügung gestellt und darf dritten Parteien nicht offen gelegt werden. ClientNet ermöglicht dem Kunden, Daten sowie den Umfang der Nutzung der Dienstleistungen einzusehen und bietet eine Reihe von Konfigurations- und Management-Einrichtungen.

5. Technischer Support

5.1. Symantec wird vierundzwanzig (24) Stunden/Tag und sieben (7) Tage/Woche:
(a) technischen Support für mit den Diensten zusammenhängenden Problemen erbringen; und
(b) sich in Zusammenarbeit mit dem Kunden bemühen, etwa entstehende Probleme zu beseitigen.

6. Kundenleistungen

6.1. Symantec wird ihren Kundendienst innerhalb der gewöhnlicher Geschäftszeiten wie folgt erbringen:
a) um Anfragen hinsichtlich der Erbringung der Dienstleistungen zu bearbeiten;
b) um Anfragen zur Änderung von betrieblichen Teilen der Dienstleistungen zu bearbeiten; und
c) um Anfragen im Hinblick auf Rechnungen und Zahlungen zu bearbeiten.
6.2 Falls in der jeweiligen Leistungsbeschreibung nicht anders angegeben, wird sich das Global Provisioning Team von Symantec bei Erhalt eines Auftrags oder Änderungsantrags, die vollkommen fertig gestellt und einklagbar sind, um die Bereitstellung des Dienstes binnen siebenundzwanzig (27) gewöhnlichen Geschäftszeiten bemühen, vorausgesetzt alle Phasen hinsichtlich der technischen verkehrsüblichen Sorgfalt wurden durchlaufen.

7. Nicht teilbare Dienst-Pakete

7.1. 7.1 Die folgende Tabelle führt nicht teilbare Dienst-Pakete auf, die in Abschnitt B „Dienste und Gebühren“ ausgewählt werden können.

Aktuelle nicht teilbare Dienst-Pakete	Einzelservices (Älterer Einzelservice)	Ältere nicht teilbare Dienst-Pakete
Symantec MessageLabs Email Protect.cloud	Email AV, Email AS	MessageLabs Email Protect
Symantec MessageLabs Email Control.cloud	Email IC, Email CC	MessageLabs Email Control
Symantec MessageLabs Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC	MessageLabs Email Safeguard (or MessageLabs Email Protect & Control)
Symantec MessageLabs Web v2 Protect & Control.cloud	Web v2 Protect, Web v2 URL	MessageLabs Web Protect & Control
Not Offered	(Email AV, Email AS, Web AVASv2)	MessageLabs Email Protect & Web Protect
Not Offered	(Email AV, Email IC, Email AS, Email CC, Web AVASv2)	MessageLabs Email Protect & Control & Web Protect
Not Offered	(Email AV, Email AS, Web AVASv2, Web URLv2)	MessageLabs Email Protect & Web Protect & Control
Symantec MessageLabs Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web v2 Protect, Web v2 URL (Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2)	MessageLabs Email & Web Safeguard (or MessageLabs Email & Web Protect & Control)
Symantec MessageLabs 2 Email Services Bundle	2 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 2 Email Services Bundle
Symantec MessageLabs 3 Email Services Bundle	3 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 3 Email Services Bundle
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving (P))	MessageLabs Email Protect & Control & Archiving (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Lite (P))	MessageLabs Email Protect & Control & Archiving Lite (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Premium(P))	MessageLabs Email Protect & Control & Archiving Premium(P)
Symantec MessageLabs Security Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2, IMSS	MessageLabs Security Safeguard
Symantec MessageLabs Complete Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud **(Für Kunden, die Dienste vor dem 1. Oktober 2011 erworben haben:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud)	MessageLabs Complete Email Safeguard
Symantec MessageLabs Complete Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud, Web v2 Protect, Web v2 URL **(Für Kunden, die Dienste vor dem 1. Oktober 2011 erworben haben:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Ar-	MessageLabs Complete Email & Web Safeguard

	chive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL)	
Symantec MessageLabs Ultimate Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud, Web v2 Protect, Web v2 URL, IMSS **(Für Kunden, die Dienste vor dem 1. Oktober 2011 erworben haben:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL, IMSS)	MessageLabs Ultimate Safeguard
Symantec Enterprise Vault.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud	MessageLabs Email Archiving L or Email Archiving.cloud (L)
Symantec Enterprise Vault Enhanced.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec EnterpriseVault Mailbox Continuity.cloud	Messagelabs Email Enhanced Archive L or Email Enhanced Archiving.cloud (L)

8. Ältere Dienstnamen

8.1 Für Kunden, die Dienste vor dem 1. Juni 2011 erworben haben, gilt Folgendes: Für die in diesem Dokument verwendeten Dienstnamen wird eine Nomenklatur verwendet, die von den ursprünglichen Namen der älteren Dienste abweicht. Die nachfolgende Tabelle enthält eine Liste der entsprechenden älteren Bezeichnungen für die überarbeitete Nomenklatur. Kunden können so feststellen, welche Abschnitte in diesem Dokument für die Services gelten, die sie unter der früheren Nomenklatur erworben haben.

Älterer Dienstname	Aktueller Dienstname
MessageLabs Email Anti-Virus	Symantec MessageLabs Email Anti-Virus.cloud
MessageLabs Email Image Control	Symantec MessageLabs Email Image Control.cloud
MessageLabs Email Anti-Spam	Symantec MessageLabs Email Anti-Spam.cloud
MessageLabs Email Content Control	Symantec MessageLabs Email Content Control.cloud
MessageLabs Boundary Encryption	Symantec MessageLabs Email Boundary Encryption.cloud
MessageLabs Web Anti-Spyware and Anti-Virus Service v2	Symantec MessageLabs Web v2 Protect.cloud
MessageLabs Web URL Service v2	Symantec MessageLabs Web v2 URL.cloud
MessageLabs Email Archiving P	Symantec MessageLabs Email Archiving.cloud (P)
MessageLabs Enterprise Instant Messenger (EIM)	Symantec MessageLabs EIM.cloud
MessageLabs EIM Connect	Symantec MessageLabs EIM Connect.cloud
MessageLabs EIM Communicate	Symantec MessageLabs EIM Communicate.cloud
MessageLabs Policy Based Encryption	Symantec MessageLabs Policy Based Encryption.cloud
MessageLabs Email Continuity (EC), or Symantec MessageLabs Email Continuity.cloud (D)	Symantec Email Continuity.cloud (EC)
Schemus Tool	Schemus Tool
MessageLabs Instant Messaging Security Service (IMSS)	Symantec MessageLabs Instant Messaging Security.cloud
MessageLabs Email Archiving D, or Symantec MessageLabs Email Archiving.cloud (D)	Symantec Email Continuity Archive.cloud
MessageLabs Email Archiving Lite D, or Symantec MessageLabs Email Archiving.cloud Lite (D)	Symantec Email Continuity Archive Lite.cloud
MessageLabs Volume Mail	Symantec MessageLabs Volume Mail
Hosted Endpoint Protection	Symantec Endpoint Protection.cloud
MessageLabs Personal Archive L or Symantec MessageLabs Email Personal Archiving.cloud (L)	Symantec Enterprise Vault Personal.cloud
MessageLabs Email Discovery Archive L, or Symantec MessageLabs Email Discovery Archiving.cloud (L)	Symantec Enterprise Vault Discovery.cloud
MessageLabs Personal Archive L for BlackBerry®, or Symantec MessageLabs Personal Archive for BlackBerry®.cloud (L)	Symantec Enterprise Vault.cloud Blackberry Option
MessageLabs Email Archiving Premiium L , or Symantec MessageLabs Email Premium Archiving.cloud (L)	AdvisorMail on Symantec.cloud™
MessageLabs Email Archiving IM Premium L, or Symantec MessageLabs Email Premium Archiving.cloud for IM (L)	AdvisorMail IM Option on Symantec.cloud™
MessageLabs Email Archiving Bloomberg Message Premium L, or Symantec MessageLabs Premium Archiving.cloud for Bloomberg	AdvisorMail Bloomberg Option on Symantec.cloud™
MessageLabs Email Archive Import Service L, or Symantec MessageLabs Email Archiving.cloud (L) Import	Symantec Enterprise Vault.cloud Data Import Option
MessageLabs Email Continuity L, or Symantec MessageLabs Email Continuity.cloud (L)	Symantec Enterprise Vault Mailbox Continuity.cloud
MessageLabs User Roaming Agent Service (“Smart Connect”)	Symantec MessageLabs Web v2 Smart Connect.cloud

Anhang 2
Dienstbeschreibungen

A Der Symantec MessageLabs Email Anti-Virus.cloud Service

1. Überblick

1.1. Der Symantec MessageLabs Email Anti-Virus.cloud Service ("AV") ist ein Internet-basiertes Email-Virus-Scanning-Dienst. Die für den Kunden eingehenden Emails sowie vom Kunden abgehenden Emails einschließlich sämtlicher Anlagen, Makros oder ausführbaren Programmen werden durch den AV-Service unter Verwendung von DNS und MX-Record Einstellungen überprüft.
1.2. Die betreffende Email sowie ihre Anlagen werden durch mehrere führende Anti-Virus-Produkte, einschließlich Symantec's eigenem heuristischen Scanner "Skeptic™" gescannt.
1.3. Fortlaufende Untersuchungen von Virusverhalten sowie fortlaufende Untersuchungen von Anti-Virus-Technologien ermöglichen Symantec eine gründliche Einsicht in die effektivsten Anti-Virus-Strategien sowie -Softwarepakete.
1.4. Ermittelt Symantec eine virusbefallene Email und ist Symantec nicht in der Lage, den Virusbefall zu beheben, wird Symantec den Kunden unverzüglich informieren und dabei ausreichende Informationen zur Verfügung stellen, damit der Kunde die virusbefallene Email erkennen und löschen kann.
1.5. Im Rahmen des AV-Service werden so viele Emails einschließlich ihrer Anlagen wie möglich gescannt. Hierbei kann es vorkommen, dass Anlagen von Emails, die vom Verwender geschützt werden, nicht gescannt werden können (z.B. Anlagen, die Passwort-geschützt und/oder verschlüsselt sind).

2. Alarm-Nachrichten

2.1. Enthält eine an den Kunden eingehende Email oder deren Anlagen einen Virus, so kann, wenn der Kunde dies wünscht, eine automatische Alarm-Meldung an den Absender sowie an den gewünschten Empfänger versendet werden. Im Hinblick auf die vom Kunden abgehenden Emails ist dieser Service nur soweit möglich, dass die Alarm-Email nur an den Absender und nicht auch an den gewünschten Empfänger versendet wird. Die befallene Email wird an einen sicheren Server weitergeleitet, der die Email innerhalb von dreißig (30) Tagen löscht. Handelt es sich bei der befallenen Email um ein Massen-Email-Virus, wird diese sofort gelöscht.
2.2. Kommt es zu einem wesentlichen Ausbruch eines neuen Virus, wird eine Alarm-Nachricht über ClientNet veröffentlicht.

3. Konfiguration

3.1. ClientNet kann dafür verwendet werden, Banner-Texte anzupassen, virusbefallene Emails zu löschen sowie den Maximalumfang von Emails einzurichten.

4. Freigabe von virusbefallenen Emails

4.1. Wird angezeigt, dass eine virusbefallene Email freigegeben werden kann, so kann die Email von dem sicheren Server unter Verwendung von ClientNet freigegeben werden. Die Email wird entweder an die ursprüngliche Adresse der Original-Empfängerliste oder an eine bestimmte, Symantec vorher mitgeteilte sowie durch Symantec in ClientNet registrierte Adresse gesendet (bitte beachten Sie: Bei diesen Adressen kann es sich um Gruppen von Emailnamen oder Pseudonymen handeln, sodass die Email an alle Adressen der Gruppe oder den Pseudonymen versendet wird). Die virusbefallene Email kann auch an eine andere Adresse versendet werden, sofern Symantec eine Freigabeermächtigung erhält. Symantec wird nur auf Anfrage des Kunden virusbefallene Emails weiterleiten. Symantec wird nicht virusbefallene Emails an den Versender der betreffenden Email zurücksenden oder an Dritte weiterleiten. Bestimmte virusbefallene Emails, die an den Kunden versendet werden, sind nicht freigabefähig, da sie wegen Virusbefalls besonders "ansteckend" sind und Schäden verursachen können. Diese Arten von Emails werden über ClientNet bekannt gegeben.

5. AV Sonderbedingungen

5.1 Wünscht der Kunde die Freigabe einer virusbefallenen Email, wird Symantec innerhalb von acht (8) gewöhnlichen Geschäftsstunden diese nach Zugang eines durch einen Vertretungsberechtigten des Kunden unterschriebenen Freigabeantrags freigeben.

B Der Symantec MessageLabs Email Image Control.cloud Service

1. Überblick

1.1. Der Symantec MessageLabs Email Image Control.cloud Service (“IC”) ist ein internet-basiertes Email-Image-Control-Service, der dazu bestimmt ist, in Bilddateien enthaltene pornografische Bilder zu erkennen. IC ist Bestandteil des Serviceumfangs, das von Symantec 24h/Tag und sieben (7) Tage/Woche erbracht wird.

2. Leistungsbeschreibung

2.1. Die an den Kunden eingehenden und vom Kunden abgehenden Emails können unter Verwendung der “Image Composition Analysis“ (ICA) nach pornografischen Bilddateien gescannt werden, die als Anlage zu Emails in Bilddateien enthalten sind.
2.2. Wird es für möglich gehalten, dass eine an den Kunden eingehende oder vom Kunden abgehende Email pornografische Bilder enthält, werden eine Reihe von Maßnahmen ergriffen, die davon abhängen, welche Konfigurationsmöglichkeiten der Kunde ausgewählt hat.

3. Konfiguration

3.1. Mit Erhalt eines vollständig ausgefüllten und von Symantec bestätigten Auftragsformulars, wird Symantec dem Kunden den Service zur Verfügung stellen. IC wird für jede Domain des Kunden aktiviert. Der Kunde ist – je nach seinem individuellen Bedarf - selbst zur Einstellung der Konfigurationsmöglichkeiten für seine Domains verantwortlich. Der Kunde wird IC unter Benutzung von ClientNet konfigurieren.
3.2. Es gibt verschiedene Möglichkeiten zur Einstellung des Erkennungsgrades, nach dem der ICA-Filter arbeitet. Erkennungsgrade können als Hoch, Mittel und Niedrig eingestellt werden. Die Einstellungsgrade gelten nur als Richtwerte. Daher werden mehr Emails bei dem Einstellungsgrad „Hoch“ und weniger Emails bei dem Einstellungsgrad „Niedrig“ erkannt.
3.3. Es gibt verschiedene Möglichkeiten zur Bestimmung von Maßnahmen, die zu ergreifen sind, wenn pornografische Bilddateien erkannt werden. Diese Möglichkeiten können für ein- und abgehende Emails unterschiedlich eingestellt werden. Sie sollten allerdings mit einer beim Kunden vorhandenen “Acceptable Computer Use Policy” (oder eines entsprechenden Dokuments) eingestellt werden. Folgende Einstellungsmöglichkeiten stehen zur Verfügung:

3.3.1 Markieren von verdächtigen Emails zur weiteren Bearbeitung (es stehen Statistiken zur Verfügung, die über ClientNet eingesehen werden können);

3.3.2 Markieren von verdächtigen Emails in der Kopfzeile („Header“) der Email (gilt nur für eingehende Emails);

3.3.3 Vervielfältigen von verdächtigen Emails auf einer vorher bestimmten Email-Adresse;

3.3.4 Umleitung von verdächtigen Emails auf eine vorher bestimmte Email-Adresse;

3.3.5 Löschung von verdächtigen Emails; und

3.3.6 Markieren von verdächtigen Emails in der Betreffzeile.

3.4 Wenn der Kunde zwecks Verwaltung von IC vertrauenswürdige Absender oder Empfänger angegeben hat, werden die E-Mails dieser Absender und Empfänger nicht von IC gescannt.

4. Versendung von Mitteilungen

4.1. Wählt der Kunde die Möglichkeiten “Umleitung” oder “Löschung” einer Email, die eine verdächtige, pornografische Bilddatei im Sinne der Ziffer 3.3 enthält, kann eine automatische Alarmnachricht an den Versender der Email gesendet werden. Handelt es sich dabei um eine an den Kunden eingehende Email kann die Alarmnachricht auch an den gewünschten Empfänger der Email versendet werden. Solche automatischen Alarmnachrichten können vom Kunden über ClientNet aktiviert und deaktiviert werden.
4.2. Mitteillungen über die Leistungsfähigkeit von IC sind über ClientNet abrufbar. Über ClientNet können Statistiken über eingehende und abgehende Emails eingesehen werden, die "verdächtig" sind, pornografische Bilddateien zu enthalten. ClientNet kann so eingestellt werden, dass Berichte erstellt und wöchentlich oder monatlich an den Kunden per Email versendet werden können.

5. Image Control Sonderbedingungen

5.1. KEINE SOFTWARE, DIE DAZU BESTIMMT IST, PORNOGRAFISCHE BILDER ZU ERMITTELN, KANN EINEN 100% ERKENNUNGSERFOLG GARANTIEREN. SYMANTEC WIRD SICH JEDOCH BESTMÖGLICH BEMÜHEN, PORNOGRAFISCHE BILDER ZU ERKENNEN. DER KUNDE NIMMT ZUR KENNTNIS, DASS DIE ERKENNUNGSQUOTE VON DEN VOM KUNDEN AUSGEWÄHLTEN EINSTELLUNGSMÖGLICHKEITEN DES IC ABHÄNGT.
5.2. Im Einzelfall kann es vorkommen, dass Anlagen, die vom Versender geschützt sind (zum Beispiel durch Passwörter und/ oder durch Verschlüsselung), nicht gescannt werden können.
5.3. IC kann nach in manchen Versionen von Word-, Excel-, PowerPoint- und pdf-Dokumenten, jedoch nicht in anderen Dokumenten eingebetteten pornographischen Bildern suchen.
5.4. Symantec weist ausdrücklich darauf hin, dass die Konfiguration von IC ausschließlich der Verantwortung des Kunden unterliegt. IC ist nur dafür bestimmt, dem Kunden zu ermöglichen, eine bereits vorhandene und verwendete „Acceptable Computer Use Policy“ (oder ein entsprechendes Dokument) zu benutzen. Die Einwilligung des betroffenen Mitarbeiters des Kunden ist - soweit erforderlich - vom Kunden sichergestellt. Die Verantwortung gegenüber den Nutzern und Betroffenen liegt allein beim Kunden. Symantec weist den Kunden deshalb ausdrücklich darauf hin, die Rechtmäßigkeit der Anwendung zu überprüfen. Der Kunde nimmt zur Kenntnis, dass der Begriff der pornografischen Bilddatei subjektiv bestimmt ist. Der Kunde sollte dies berücksichtigen, wenn er die Dienstleistungen entsprechend einstellt. Symantec übernimmt keine Haftung für die zivilrechtliche oder strafrechtliche Haftung des Kunden wegen seiner Verwendung des IC Services.
5.5. Gibt der Kunde ein virusbefallenes Email frei oder beantragt er eine Freigabe, wird die freigegebene Email von IC nicht vor der entsprechenden Freigabe gescannt.

C Der Symantec MessageLabs Email Anti-Spam.cloud Service

1. Übersicht

1.1. Der Symantec MessageLabs Email Anti-Spam.cloud Service (“AS”) ist ein internet-basierter Email-Anti-Spam-Dienst, der dazu bestimmt ist, den Kunden vor unerwünschten Emails (UCE/UCB) zu schützen. AS ist Bestandteil des Serviceumfangs, welcher von Symantec 24h/Tag und sieben (7) Tage/Woche erbracht wird.

2. Leistungsbeschreibung

2.1. Beim Kunden eingehende Emails können unter Verwendung verschiedener Methoden gescannt werden, um festzustellen, ob es sich um Spam handelt oder nicht. Wird eine eingehende Email Spam-Mail identifiziert, werden eine Reihe von Maßnahmen ergriffen, die davon abhängen, welche Konfigurationsmöglichkeiten der Kunde ausgewählt hat. Die Konfigurationsmöglichkeiten sind unten in Ziffer 3.2 beschrieben und können vom Kunden über ClientNet abgerufen werden.

2.2 Der Kunde oder ein einzelner Nutzer, falls der Kunde Einstellungen auf Nutzerebene aktiviert hat, kann eine sog. “Whitelist” erstellen. Wird diese ausgewählt und geht eine Email von einer Domain aus dieser “Whitelist” ein, hebt diese Freigabe automatisch jede sonstige Methode zur Erkennung von Spam auf.

2.3 Der Kunde oder ein einzelner Nutzer, falls der Kunde Einstellungen auf Nutzerebene aktiviert hat, kann eine sog. “Blacklist” erstellen. Wird diese ausgewählt und geht eine Email von einer Domain aus dieser “Blacklist” ein, wird diejenige Maßnahme durchgeführt, die der Kunde unten in Ziffer 3.2 als Konfigurationsmöglichkeit ausgewählt hat.

2.4 Eine Reihe von öffentlichen ”Blacklists” kann ausgewählt werden. Wird diese Erkennungsmethode ausgewählt und geht eine Email von einer Domain aus einer dieser öffentlichen “Blacklists” ein, wird diejenige Maßnahme durchgeführt, die der Kunde unten in Ziffer 3.2 als Konfigurationsmöglichkeit ausgewählt hat.

2.5 Wird die Email durch oben erwähntes Blacklisting nicht gelöscht, und ist die strengere, vom Kunden gewählte Signatur-basierte Erkennungsmethode ausgewählt, so wird die Email gemäß der Signatur-basierten Erkennungsmethode bewertet. Wir die E-Mail demzufolge als Spam erkannt, erfolgt die gemäß der in 3.2 beschriebenen Konfigurations-Optionen bestimmte Maßnahme. Diese Maßnahme gilt vorrangig vor anderen weniger strengen Maßnahmen, welche zuvor durch etwaige Blacklisting Methoden definiert wurden.

2.6 Führen die oben beschriebenen Anwendungsmethoden nicht dazu, dass die Email gelöscht wird und hat der Kunde eine strengere heuristische Erkennungsmethode ausgewählt,, werden die an den Kunden eingehenden Emails unter Verwendung des heuristischen Scannens gescannt. Wird eine Email nach der heuristischen Erkennungsmethode als Spam erkannt, werden die unten in Ziffer 3.2 beschriebenen Maßnahmen durchgeführt. Diese Maßnahme gilt vorrangig vort jeder weniger aufwendigen, oben beschriebenen Erkennungsmethode.

2.7 Von Symantec zur Verfügung gestellte ”Blacklists” und ”Whitelists” gelten nur als Beispiele.

3. Konfiguration

3.1. Mit Erhalt eines vollständigen und angenommenen Auftrags wird Symantec Email AS für den Kunden aktivieren. Am Anfang wird Email AS für alle Domänen des Kunden aktiviert. DER KUNDE IST SICH DESSEN BEWUSST, DASS EMAIL AS VON ANFANG AN UNTER ANWENDUNG DER SYMANTEC-STANDARDEINSTELLUNGEN BEREITGESTELLT WIRD UND DASS DER KUNDE FÜR DIE KONFIGURATION VON EMAIL AS ÜBER CLIENTNET ABGESTIMMT AUF SEINE EIGENEN ERFORDERNISSE ALLEIN VERANTWORTLICH IST. Die bezüglich Email AS angewendeten Standardeinstellungen umfassen folgende Aktionen:

3.1.1 Blockieren und Löschen von E-Mails; oder
3.1.2 In-Quarantäne-Stellen von E-Mails; und
3.1.3 Einsatz einer "Whitelist" für IP-Adressen, Domänen und E-Mail-Adressen; und
3.1.4 Einsatz von vorausschauender Spam-Erkennung (Skeptic).

3.2. Es gibt verschiedene Möglichkeiten, die Maßnahmen zu bestimmen, wenn eine Email als Spam erkannt wird. Diese Möglichkeiten, die unten aufgeführt sind, können vom Kunden für die jeweilige zur Verfügung stehende Erkennungsmethode ausgewählt werden:

3.2.1 Markierung von verdächtigen Emails in der Kopfzeile (“Header”) der Email
3.2.2 Markierung von verdächtigen Emails in der Betreffszeile der Email
3.2.3 Umleitung von verdächtigen Emails auf eine vorher bestimmte Email-Adresse
3.2.4 Löschung von verdächtigen Emails
3.2.5 Spam Quarantäne.

4. Spam Quarantäne Leistungsbeschreibung

4.1. Falls der Kunde Spam Quarantäne für eine Domain aktiviert, wird für jeden Benutzer automatisch ein Spam Quarantäne Account eingerichtet, sobald der AS Service für diesen Benutzer die erste Spam-Email identifiziert hat. Der Benutzer erhält dann automatisch ein Email-Benachrichtigung.
4.2. Die Benutzer können auf ihre Spam Quarantäne mittels dem webbasierten Spam Manager interface zugreifen.
4.3. Die Spam Quarantäne Infrastruktur befindet sich physikalisch in Großbritannien.
4.4. Potentielle Spam E-Mails werden in der Spam Quarantäne maximal 14 Tage lang gespeichert und danach automatisch gelöscht. Der Kunde kann gegen Zahlung einer Zusatzgebühr, die sich nach der Anzahl der Benutzer und Tage berechnet, eine Verlängerung der normalen Speicherdauer von vierzehn (14) Tagen erwerben („Symantec MessageLabs Extended Spam Quarantine“).
4.5. Sollte die Spam Quarantäne die potentielle Spam E-Mail nicht annehmen können, wird diese E-Mail markiert (“tagged”) und an den Empfänger zugestellt.

5. Spam Quarantäne Konfiguration

5.1. Der Kunde konfiguriert die Spam Quarantäne mit dem ClientNet Web-Interface.
5.2. Die Standard-Einstellung für Benachrichtigungen ist auf 5.2.1 eingestellt (täglich, s.u.). Der Benutzer kann jederzeit eine der folgenden Einstellungen auswählen:

5.2.1. tägliche Benachrichtigung;

5.2.2. Benachrichtigung in frei definierten Intervallen;

5.2.3. keine Benachrichtigungen.

5.3. Spam Manager bietet die folgenden Freigabe-Optionen:

5.3.1. E-Mail löschen;

5.3.2. E-Mail an ursprüngliche Ziel-Adresse zustellen;

5.3.3. Text der E-Mail ansehen.

5.4. Zur Nutzung der Funktion „Spam-Quarantäne" muss der Kunde eine Überprüfungsliste bei Symantec hinterlegt haben. Die Überprüfungsliste enthält alle vom Kunden genutzten gültigen E-Mail-Adressen. Alle Empfängeradressen, die nicht auf der Überprüfungsliste stehen, gelten als ungültig und es wird keine E-Mail an diese Adresse zugestellt.

5.5. Mit dem ClientNet Web-Interface kann ein Kunden verschiedene Aspekte des Spam Manager Dienstes kontrollieren:> (a) automatisierte oder manuelle Benachrichtigungen; (b) zusammenfassende Benachrichtigungen, (c) Sprach-Einstellungen; (d) Einstellungen auf Nutzerebene; (e) vordefinierte E-Mail Aliase und (f) besondere Benutzer-Rechte (z.B. Quarantäne Administratoren).

5.6. Der Kunde darf im Hinblick auf eine Spam-Quarantäne E-Mail-Adressgruppen einrichten, um für den Zweck eines E-Mail-Aliasing und delegierten Zugangs eine Reihe einzelner E-Mail-Adressen mit einer ‚Inhaber'-E-Mail-Adresse zu verknüpfen. Maximal dürfen hierbei fünfzig (50) E-Mail-Adressen mit einer E-Mail-Hauptadresse verknüpft werden. Symantec behält sich das Recht vor, die Kontogruppe bzw. die Aliasing-Verknüpfungen des Kunden zu entfernen, wenn diese Höchstzahl überschritten wird.

6. Versendung von Berichten

6.1. Berichte über die Leistungsfähigkeit von AS sind über ClientNet abrufbar. ClientNet kann so eingestellt werden, dass Berichte erstellt und wöchentlich oder monatlich an den Kunden per Email versendet werden können.

7. Anti Spam Sonderbedingungen

7.1. KEINE ANTI-SPAM-SOFTWARE KANN EINEN 100% ERKENNUNGSERFOLG GARANTIEREN. SYMANTEC WIRD SICH JEDOCH BESTMÖGLICH BEMÜHEN, SPAM ZU ENTDECKEN. DER KUNDE NIMMT ZUR KENNTNIS, DASS DIE ERKENNUNGSQUOTE VON DEN VOM KUNDEN AUSGEWÄHLTEN EINSTELLUNGSMÖGLICHKEITEN DES AS ABHÄNGT.

7.2. Symantec weist ausdrücklich darauf hin, dass die Konfiguration von AS ausschließlich der Verantwortung des Kunden unterliegt. AS empfiehlt die Verwendung einer Nutzungsbestimmung („Acceptable Computer Use Policy" oder ein entsprechendes Dokument). Die Einwilligung der betroffenen Mitarbeiter des Kunden wird - soweit erforderlich- vom Kunden sichergestellt. Die Verantwortung gegenüber den Nutzern und Betroffenen liegt allein beim Kunden. Symantec weist den Kunden deshalb ausdrücklich darauf hin, die Rechtmäßigkeit der Anwendung des AS zu überprüfen. Symantec übernimmt keine Haftung für die zivilrechtliche oder strafrechtliche Haftung des Kunden wegen seiner Verwendung des AS Services.

D Der Symantec MessageLabs Email Content Control.cloud Service

1. Übersicht

1.1. Der Symantec MessageLabs Email Content Control.cloud Service (der „Content Control Service“) ist ein Dienst von Symantec, welcher dem Kunden die Möglichkeit bietet, eine auf Regeln basierte und ihren Nutzungsbestimmungen für E-Mail („AUP“) entsprechende Filterstrategie zu konfigurieren. Dieser Dienst ist Bestandteil des Serviceumfangs, welcher von Symantec 24h/Tag und sieben (7) Tage/Woche erbracht wird.

2. Leistungsbeschreibung

2.1. Der Content Control Service ermöglicht es dem Kunden, ein Regelwerk zu erstellen, nach dem beim Kunden ein- und ausgehende Emails gefiltert werden. Eine Regel ist eine vom Kunden erstellte Anweisung, mit deren Hilfe bestimmte Formate von Nachrichten und Anhängen sowie Inhalte identifiziert werden, und der Umgang mit dieser Email gemäß Kundenvorgaben bestimmt wird.

3. Konfiguration

3.1. Mit Erhalt einer unterzeichneten Vertragsänderung, wird Symantec dem Kunden den Content Control Service für jede zutreffende Domain aktivieren. Der Kunde ist – je nach seinem individuellen Bedarf - selbst zur Einstellung der Konfigurationsmöglichkeiten für seine Domains verantwortlich. Der Kunde wird den Content Control Service unter Verwendung von ClientNet, einem webbasierten Management Interface, konfigurieren.

3.2. Der Kunde darf die Regeln auf ‘pro Domain’, ‘pro Gruppe’ oder ‘Individueller’ Basis konfigurieren.

3.3. Die Regeländerungen des Kunden werden innerhalb von 24 Stunden aktiv.

3.4. Es gibt verschiedene Möglichkeiten zur Bestimmung von Maßnahmen, die zu ergreifen sind, wenn verdächtige Emails erkannt werden. Diese Möglichkeiten können für ein- und abgehende Emails unterschiedlich eingestellt werden. Sie sollten allerdings mit einer beim Kunden vorhandenen Nutzungsbestimmung (“Acceptable Computer Use Policy” oder ein entsprechendes Dokument) eingestellt werden. Folgende Einstellungsmöglichkeiten stehen zur Verfügung:

3.4.1 Blockieren und Löschen von verdächtigen Emails,

3.4.2 Markieren (gilt nur für eingehende Emails) und Umleitung von verdächtigen Emails an den angegebenen Administrator,

3.4.3 Markieren (gilt nur für eingehende Emails) und Versand einer Kopie von verdächtigen Emails an den angegebenen Administrator,

3.4.4 Markieren von verdächtigen Emails in der Kopfzeile („Header“) der Email (gilt nur für eingehende Emails),

3.4.5 Kompression der Email-Anhänge,

3.4.6 Mitloggen (Protokollieren) zur Erstellung von Statistiken welche über ClientNet eingesehen werden können;

3.4.7 Markierung von verdächtigen Emails in der Betreffszeile der Email.

4. Versendung von Mitteilungen

4.1. Über ClientNet kann der Kunde das Resultat der Regeln durch tägliche, wöchentliche, monatliche oder jährliche Zusammenfassungen auswerten. Die Zusammenfassungen sind nach Regeln und Benutzern sortiert.

4.2. Auf Wunsch werden Berichte mit Daten über die Aktivität der genutzten Dienste wöchentlich oder monatlich erstellt und an den Kunden per Email übersandt.

4.3. Über ClientNet kann der Kunde Benachrichtigungen, die er auf Per-Rule-Basis konfiguriert hat, aktivieren und deaktivieren.

5. Content Control Support

5.1. Der Support beinhaltet Schulung auf dem Content Control Web-Interface inkl. einer Dienstebeschreibung und Frage-Antwort-Sessions.

6. Wildcarding

6.1 Content Control funktioniert auf Basis eines exakten Abgleichs mit den vom Kunden konfigurierten Regeln. Als besondere Ausnahme macht es Wildcarding dem Kunden jedoch möglich, Content Control über ClientNet zu konfigurieren, um bestimmte alphanumerische Formeln zu ermitteln, die einem besonderen Muster folgen (z. B. Sozialversicherungsnummern und Kreditkarteninformationen).

7. Content Control Sonderbedingungen

7.1. Die von Symantec gestellten bzw. vorgeschlagenen Wortlisten enthalten Wörter die als anstößig gesehen werden könnten. Der Kunde ist für die Zugänglichmachung dieser Listen an die Nutzer verantwortlich.

7.2. Symantec darf Standardwortlisten erstellen und veröffentlichen, die Worte enthalten, welche aus den Spezialwortlisten von dem Kunden gewonnen werden.

7.3. Wenn der Content Control Service zusammen mit der Block-Funktion des Anti-Spam Services benutzt wird, ist es möglich, dass verdächtiger Spam blockiert wurde, bevor die Email von dem Content Control Service gefiltert wird.

7.4. Der Content Control Service kann nach in manchen Versionen von Word-, Excel-, PowerPoint- und pdf-Dokumenten, jedoch nicht in anderen Dokumente suchen.

7.5. Symantec weist ausdrücklich darauf hin, dass die Konfiguration von dem Content Control Service ausschließlich der Verantwortung des Kunden unterliegt. Die Genauigkeit der Konfiguration bestimmt die Genauigkeit des Content Control Services und deshalb übernimmt Symantec keine Haftung für Schäden oder Verluste die direkt oder indirekt aus der Ablehnung von Emails mit verdächtigem Inhalt oder Emails mit fehlerhaft identifizierten Inhalten resultieren, wenn anschließend festgestellt wird, dass die Email keinen verdächtigen Inhalt hatte.

7.6. Symantec empfiehlt, dass der Kunde eine Nutzungsbestimmung („Acceptable Computer Use Policy“ oder ein entsprechendes Dokument) hat, um die Benutzung von Email zu kontrollieren. Die Einwilligung der betroffenen Mitarbeiter des Kunden wird - soweit erforderlich- vom Kunden sichergestellt. Die Verantwortung gegenüber den Nutzern und Betroffenen liegt allein beim Kunden. Symantec weist den Kunden deshalb ausdrücklich darauf hin, die Rechtmäßigkeit der Anwendung des Content Control Services zu überprüfen. Symantec übernimmt keine Haftung für die zivilrechtliche oder strafrechtliche Haftung des Kunden wegen seiner Verwendung des Content Control Services.

E Symantec MessageLabs Email Boundary Encryption.cloud Service (Verschlüsselungsdienst)

1. Übersicht

1.1. Der Symantec MessageLabs Email Boundary Encryption.cloud Service ("BE") von Symantec bietet verschlüsselte Kommunikationskanäle, die dem Kunden die Bildung eines sicheren, privaten E-Mail-Netzwerks (Secure Private Email Network, SPEN) mit benannten Partnerorganisationen (die "SPEN-Partner") ermöglichen. Diese Konfiguration ist als die Verschlüsselung „Enforced" bekannt.
1.2. Darüber hinaus kann der Kunde auch verschlüsselte E-Mails empfangen, die opportunistisch von Organisationen gesendet werden, welche über TLS-fähige Mail-Server verfügen, für die keine Verschlüsselung "Enforced" in Bezug auf den Kunden vorhanden ist, wenn diese Organisationen über TLS-fähige Mail-Server verfügen. Diese Konfiguration ist als die Verschlüsselung „Opportunistic" bekannt.
1.3. Falls der Kunde BE abonniert, jedoch nicht ausdrücklich SPEN-Partner identifiziert hat, kann der Kunde E-Mails empfangen, die opportunistisch über TLS ankommend (Inbound) gesendet werden, und opportunistisch verschlüsselte E-Mails ausgehend (Outbound) an Nicht-SPEN-Partner-Organisationen senden.

1.4. Der Kunde kann auch seine E-Mail-Server für das BE-Modell „Secure Connection" (Sichere Verbindung) konfigurieren. In diesem Fall gilt:

1.4.1 Der Austausch von E-Mails zwischen Symantec und den mit „Secure Connection" betriebenen Mail-Servern des Kunden wird durch TLS-Verschlüsselung gesichert. Ob das weitergehende Routing in nicht-verschlüsseltem oder verschlüsseltem Format durchgeführt wird, hängt ab (i) von den durch den Kunden festgelegten TLS-Erzwingungen und (ii) von der Fähigkeit des Zielservers zum Empfang von E-Mails über Opportunistic TLS.

1.4.2 **DER KUNDE ANERKENNT UND AKZEPTIERT, DASS BEI NICHTANWENDUNG DES MODELLS „SECURE CONNECTION" AUF EINEN BESTIMMTEN MAIL-SERVER DIE EINGEHENDEN UND ABGEHENDEN E-MAILS DES KUNDEN, DIE VON DIESEM MAIL-SERVER STAMMEN ODER DURCH DIESEN EMPFANGEN WERDEN, NICHT DURCH TLS-VERSCHLÜSSELUNG GESICHERT SIND. DEMENTSPRECHEND ANERKENNT UND AKZEPTIERT DER KUNDE, DASS ER KEINE SENSITIVEN DATEN ÜBER SOLCHE MAIL-SERVER SENDEN ODER EMPFANGEN DARF UND BEI NICHTBEACHTUNG DIESES HINSWEISES DAS ALLEINIGE RISIKO TRÄGT**.

1.5 Falls der Kunde BE in Verbindung mit dem PBE Service verwendet, besteht die von Symantec empfohlene bestgeeignete Vorgehensweise für den Kunden darin, das BE-Modell „Secure Connection" auf allen seinen Mail-Servern zu implementieren.
1.6 BE FUNKTIONIERT NUR BEI DER VERWENDUNG ZUSAMMEN MIT EINEM DER DIENSTE EMAIL AV, EMAIL AS, EMAIL IC UND/ODER EMAIL CC UND KANN NICHT ALS EIGENSTÄNDIGER DIENST FUNKTIONIEREN.

2. Serviceleistungen und Rechnungsstellung

2.1. Symantec beginnt mit der Rechnungsstellung für BE ab dem Datum, an dem Symantec bestätigt, dass das Netzwerk des Kunden technisch in der Lage ist, BE zu unterstützen ("technisches Genehmigungsdatum").
2.2 Klausel 5.2 in Anhang 1 kann nicht auf BE angewendet werden. Symantec setzt sich zum Ziel, BE-Bestellungen und -Änderungsanforderungen innerhalb von vier Wochen ab dem technischen Genehmigungsdatum auszuführen, vorausgesetzt, dass der Kunde alle Ermittlungen in Bezug auf das Vertragsobjekt mit der gebotenen Sorgfalt geführt hat.
2.3 Falls Symantec zur BE-Bereitstellung zusätzliche technische Ressourcen bereitstellen muss, weil der Kunde nicht die erforderlichen Due-Diligence-Vorgaben erfüllt hat, behält Symantec sich das Recht vor, zusätzliche Gebühren für gewerbliche Dienstleistungen zu einem Satz von €1500 pro Person pro Tag in Rechnung zu stellen.

3. Konfiguration

3.1. Der Kunde definiert die SPEN-Partner, mit denen er über eine Domäne sicher kommunizieren möchte. Die SPEN-Partner können Kunden oder Nichtkunden von BE sein, jedoch unterstützt Symantec SPEN-Partner nicht direkt. Nicht-SPEN-Partnerorganisationen können E-Mails über Opportunistic Outbound TLS, wie in Klausel 1 oben beschrieben, empfangen, wenn ihre Mail-Server den Empfang verschlüsselter Mails unterstützen.

3.2. BE basiert auf dem Standard 'SMTP über TLS' (Simple Mail Transfer Protocol über Transport Layer Security) ("STARTTLS").

3.3. Damit BE genutzt werden kann, müssen sowohl der Mail-Server des Kunden als auch der Mail-Server des SPEN-Partners STARTTLS unterstützen.

3.4. BE wird von ausgewählten Türmen unterstützt, über die alle STARTTLS-E-Mails geleitet werden. Dementsprechend benennt der Kunde die Domänen, welche BE nutzen sollen.

3.5. Falls BE in Verbindung mit der Signatursystemfunktion von Email AS genutzt wird, empfiehlt Symantec, dass der Kunde alle Domänen seiner SPEN-Partner in die Liste seiner Email-AS-genehmigten E-Mail-Absender einbezieht. Wenn diese empfohlene Verfahrensweise nicht befolgt wird, akzeptiert der Kunde, dass unter bestimmten Umständen, bei denen die Nichtverfügbarkeit des lokalen Signatursystems auftritt, die E-Mail über ein öffentliches Netzwerk zu einem entfernten Signatursystem umgeleitet wird.

4. Zertifikate und Authentifizierung

4.1. Wenn der Kunde eine STARTTLS-Verbindung herstellt, muss der akzeptierende Mail-Server zur Authentifizierung sein Zertifikat vorlegen. Wenn der akzeptierende Mail-Server die Authentifizierung des Dienstes wünscht, so wird Symantec sein Client-Zertifikat zur Authentifizierung vorlegen. Wenn der akzeptierende Mail-Server die E-Mail nicht authentifizieren kann, wird die E-Mail an den Kunden zurückgesendet.

4.2. Wenn ein externer Mail-Server eine STARTTLS-Verbindung herstellt, wird der Dienst sein Serverzertifikat zur Authentifizierung vorlegen, jedoch nicht darauf bestehen, dass der externe Mail-Server sein Client-Zertifikat zur Authentifizierung vorlegt.

4.3. Die Validierung eines Zertifikats obliegt der Zertifizierungsstelle (Certificate Authority), die das Zertifikat signiert hat. Für jedes von einem entfernten Mail-Server als Teil einer STARTTLS-Verbindung unterbreitete Zertifikat wird der Dienst bestätigen, dass eine anerkannte Zertifizierungsstelle (Certificate Authority) das Zertifikat signiert hat. Wenn ein Zertifikat nicht von einer anerkannten Zertifizierungsstelle (Certificate Authority) validiert werden kann, wird die Verbindung abgebrochen und die E-Mail an den Absender zurückgesendet.

5. Verschlüsselung Geschäftsbedingungen

5.1. Symantec kann keine Haftung dafür übernehmen, dass der Kunde oder ein Dritter (insbesondere SPEN-Partner) seine Pflichten bezüglich der Registrierung von Zertifikaten nicht erfüllt. Symantec kann darüber hinaus keine Haftung für das rechtzeitige Vorliegen oder die Richtigkeit dieser Informationen übernehmen.

5.2. BE ist nur zu dem Zweck vorgesehen, dem Kunden die Durchführung einer bestehenden, wirksam implementierten akzeptablen Computernutzungsrichtlinie (oder deren Entsprechung) zu ermöglichen. In manchen Ländern kann die Nutzung verschlüsselter Dienste gesetzlich geregelt sein. Dem Kunden wird geraten, vor dem Einsatz von BE stets die einschlägigen Gesetze zu prüfen. Symantec kann keine Haftung für eine zivil- oder strafrechtliche Haftung des Kunden infolge der Nutzung von BE übernehmen.

F Der Symantec MessageLabs Web v2 Protect.cloud

1. Übersicht

1.1. Sobald die relevanten Konfigurationsänderungen erfolgt sind, werden Anforderungen von Webseiten und Anhängen elektronisch über den Symantec MessageLabs Web v2 Protect.cloud Service ("Web v2 Protect") geleitet und digital untersucht.

2. Leistungsbeschreibung

2.1. Die externen HTTP- und FTP-over-HTTP-Anforderungen des Kunden, einschließlich alle Anhänge, Makros oder ausführbaren Dateien werden über den Dienst geleitet.

3. Konfiguration

3.1. Die erforderlichen Konfigurationseinstellungen, um diesen externen Datenverkehr über den Dienst umzuleiten, werden vom Kunden durchgeführt bzw. aufrechterhalten und hängen von der technischen Infrastruktur des Kunden ab. Der Kunde sollte sicherstellen, dass der interne HTTP/FTP-over-HTTP-Datenverkehr (z.B. zum Intranet des Unternehmens) nicht über den Dienst umgeleitet wird. Wenn der Kunde Internet-Dienste hat, die eine direkte Verbindung nutzen (anstatt über einen Proxyserver), ist der Kunde dafür verantwortlich, die notwendigen Änderungen an seiner eigenen Infrastruktur vorzunehmen.

3.2. Der Zugang zu dem Dienst ist über sog. Scanning-IPs beschränkt, d.h. über die IP-Adresse(n), über die der Web-Datenverkehr des Kunden erfolgt. Die Scanning-IPs werden auch zur Identifizierung des Kunden und zur dynamischen Auswahl von kundenspezifischen Einstellungen verwendet.

3.3. Web v2 Protect wird entsprechende Teile der Webseite und ihren Anhängen scannen, die Viren, boswilliger Code, Spyware oder Adware enthalten könnten. Das Scannen von bestimmten Webseiten, Inhalten oder Anhängen ist u.U. nicht möglich (zum Beispiel, wenn sie mit einem Passwort geschützt sind). Bestimmte Anhänge, die als nicht scanfähig erkannt werden, werden nicht blockiert. Der gestreamte und verschlüsselte Datenverkehr (d.h. Streaming Media und/oder HTTPS/SSL) kann nicht gescant werden und wird Web v2 Protect ungescannt passieren.

3.4. Der Roaming User Support ist eine optionale Funktion, die den Web v2 Protect Service auf Benutzer ausdehnt, die sich nicht innerhalb des Unternehmensnetzwerks befinden (z. B. auf einen Benutzer, der zuhause arbeitet). Der Kunde muss eine PAC-Datei auf dem Benutzer-PC installieren, damit der Benutzer beim Starten des Browsers auf das Web-Portal von Symantec geleitet wird. Zum Zugriff auf das Web-Portal muss der Benutzer ein Passwort und einen Benutzernamen eingeben. Eine Vorlage für die PAC-Datei kann vom ClientNet heruntergeladen und durch den Kunden modifiziert werden.

4. Alarmmeldungen

4.1. Wenn auf einer Webseite oder in Dateianhängen des Kunden ein Virus, Spyware oder Adware identifiziert wird, dann wird der Zugang zur Webseite oder dem Anhang verwehrt und dem Internet-Nutzer wird automatisch eine Alarm-Meldung als Webseite angezeigt. In seltenen Fällen, und wenn ein oder mehrere Elemente der angeforderten Inhalte blockiert sind, ist es u.U. möglich, dass Alarm-Meldung als Webseite nicht angezeigt werden kann und die angeforderten Inhalte deshalb durch die Warnmeldung ersetzt werden können. Ungeachtet davon bleibt der Zugang zur infizierten Seite oder zum infizierten Anhang verwehrt.

4.2. ClientNet ermöglicht es dem Kunden, einen Teil der automatischen Alarm-Meldung auf der Webseite individuell einzustellen.

5. Berichte

5.1 Berichte über die Leistungsfähigkeit von Web v2 Protect sind über ClientNet abrufbar.

5.2. Um Berichte über User oder Gruppen zu ermöglichen, muss der Kunde die hierfür erforderliche Softwareanwendung (den "Client Site Proxy") gemäß den Installationsrichtlinien installieren, die mit dem Client Site Proxy ausgeliefert werden. Die Nutzung dieser Software richtet sich nach der End-User-Lizenzvereinbarung, die mit dem Client Site Proxy ausgeliefert wird.

5.3 Der Kunde erkennt an, dass detaillierte ClientNet-Berichterstellungsdaten nur für einen Zeitraum von maximal vierzig (40) Tagen gespeichert werden und nach Ablauf dieses Zeitraums nicht mehr für den Kunden verfügbar sind. Zusammenfassende ClientNet-Daten sind für einen Zeitraum von maximal zwölf (12) Monaten verfügbar.

5.4 Der Kunden kann für den detaillierten ClientNet-Bericht einen verlängerten Berichterstellungszeitraum von bis zu sechs (6) Monaten anfordern, indem er WSS Enhanced Data Retention abonniert.

6. Web v2 Protect Sonderbedingungen

6.1. KEINE WEB-SCANNING-SOFTWARE KANN EINEN 100%IGEN ERKENNUNGSERFOLG GARANTIEREN. SYMANTEC WIRD SICH JEDOCH BESTMOGLICH BEMUHEN, VIREN, BOSWILLIGER CODE, SPYWARE ODER ADWARE AUFZUSPUREN. DER KUNDE NIMMT ZUR KENNTNIS, DASS DIE ERKENNUNG VON DEN VOM KUNDEN AUSGEWAHLTEN EINSTELLUNGSMOGLICHKEITEN, VON DER BEKANNTHEIT NEUER TECHNIKEN UND SONSTIGEN UNWAGBARKEITEN ABHANGEN KANN, WELCHE IN SELTENEN AUSNAHMEFALLEN DIE ERKENNUNG VERHINDERN KONNEN. SYMANTEC KANN GRUNDSATZLICH FUR HIERAUS ENTSTEHENDE SCHADEN ODER VERLUSTE NICHT EINSTEHEN UND HAFTET NUR NACH DEN VORSCHRIFTEN DIESES VERTRAGES.

6.2. Symantec weist ausdrücklich darauf hin, dass die Konfiguration von Web v2 Protect ausschließlich der Verantwortung des Kunden unterliegt. Web v2 Protect ist nur dazu gedacht, dem Kunden bei der Durchsetzung von Nutzungsbestimmungen („Acceptable Computer Use Policy" oder entsprechender Dokumente) zu unterstützen. Die Einwilligung der betroffenen Mitarbeiter des Kunden wird - soweit erforderlich- vom Kunden sichergestellt. Die Verantwortung gegenüber den Nutzern und Betroffenen liegt allein beim Kunden. In manchen Ländern kann die Nutzung von der Zustimmung einzelner Personen abhängen; dem Kunden wird deshalb geraten, vor dem Einsatz von Web v2 Protect stets die örtlich geltenden Gesetze zu prüfen. Symantec haftet nicht für die zivil- oder strafrechtlichen Folgen des Betriebs von Web v2 Protect für den Kunden.

6.3 Der Web-Datenverkehr (Traffic) des Kunden bei der Nutzung von Web v2 Protect darf dreißig Megabyte (30 MB) je Benutzer und Tag nicht überschreiten (berechnet als Durchschnitt pro Nutzer in Bezug auf die gesamte vereinbarte Nutzungsumfang des Kunden für Web v2 Protect). Für den Fall, dass dieser Tagesgrenzwert überschritten wird, behält sich Symantec folgende Maßnahmen vor:

6.3.1 Verweigerung der Bereitstellung oder vorübergehende Einstellung von Web v2 Protect im Ganzen oder in Teilen mit sofortiger Wirkung bis zum Unterbleiben der übermäßigen Nutzung; oder

6.3.2 Aufforderung der Kunden zum Erwerb eines zusätzlichen Nutzerkontingents entsprechend dem tatsächlichen Web-Datenaufkommen des Kunden und Ausstellung zusätzlicher Rechnungen und/oder Anpassung nachfolgender Rechnungen, sodass die Gebühren für die Erhöhung des angemeldeten Nutzungsaufkommens anteilmäßig für den verbleibenden Teil des laufenden Rechnungszeitraums gedeckt werden.

G Der Symantec MessageLabs Web v2 URL.cloud Service

1. Übersicht

1.1. Sobald die relevanten Konfigurationsänderungen erfolgt sind, werden Anforderungen von Webseiten und Anhängen elektronisch über den Symantec MessageLabs Web v2 URL.cloud Service ("Web v2 URL") geleitet und digital untersucht.

2. Leistungsbeschreibung

2.1. Die externen HTTP- und FTP-over-HTTP-Anforderungen des Kunden, einschließlich aller Anhänge, Makros oder ausführbaren Dateien werden über den Dienst geleitet.

3. Konfiguration

3.1. Die Konfigurationseinstellungen, die erforderlich sind, um diesen externen Datenverkehr über den Dienst zu leiten, werden vom Kunden durchgeführt bzw. aufrechterhalten und hängen von der technischen Infrastruktur des Kunden ab. Der Kunde sollte sicherstellen, dass der interne HTTP/FTP-over-HTTP-Datenverkehr (z.B. zum Intranet des Unternehmens) nicht über den Dienst läuft. Wenn der Kunde Internet-Dienste hat, die eine direkte Verbindung nutzen (anstatt über einen Proxyserver), ist der Kunde dafür verantwortlich, die notwendigen Änderungen an seiner eigenen Infrastruktur vorzunehmen.

3.2. Der Zugang zu dem Dienst ist über sog. Scanning-IPs beschränkt, d.h. über die IP-Adresse(n), aus denen der Web-Datenverkehr des Kunden kommt. Die Scanning-IPs werden auch zur Identifizierung des Kunden und zur dynamischen Auswahl von kundenspezifischen Einstellungen verwendet.

3.3. Der Kunde kann Web v2 URL konfigurieren, um die Richtlinien für die Zugangsbeschränkung zu bestimmen (die sowohl auf Kategorien als auch auf Typen von Inhalten abgestellt sein können). Der in Ziffer 5.1 beschriebene Client Site Proxy ermöglicht es dem Kunden, die Richtlinien für die Zugangsbeschränkung zu bestimmten Zeiten auf spezifische User oder Gruppen anzuwenden.

3.4 DER KUNDE IST SICH DESSEN BEWUSST, DASS WEB V2 URL VON ANFANG AN UNTER ANWENDUNG DER SYMANTEC-STANDARDEINSTELLUNGEN BEREITGESTELLT WIRD UND DASS DER KUNDE FÜR DIE KONFIGURATION VON WEB V2 URL ÜBER CLIENTNET ABGESTIMMT AUF SEINE EIGENEN ERFORDERNISSE ALLEIN VERANTWORTLICH IST. Die Standardeinstellungen umfassen eine Funktion „Blockieren und Protokollieren" für folgende URL-Kategorien:

3.4.1 Erwachsene / Eindeutig sexuell; und
3.4.2 Spyware; und
3.4.3 Spam-URLs; und
3.4.4 Kriminelle Tätigkeit.

3.5 Der Roaming User Support ist eine optionale Funktion, die den Web v2 URL Service auf Benutzer ausdehnt, die sich nicht innerhalb des Unternehmensnetzwerks befinden (z. B. auf einen Benutzer, der zuhause arbeitet). Der Kunde muss eine PAC-Datei auf dem Benutzer-PC installieren, damit der Benutzer beim Starten des Browsers auf das Web-Portal von Symantec geleitet wird. Zum Zugriff auf das Web-Portal muss der Benutzer ein Passwort und einen Benutzernamen eingeben. Eine Vorlage für die PAC-Datei kann vom ClientNet heruntergeladen und durch den Kunden modifiziert werden.

4. Alarmmeldungen

4.1. Wenn ein Benutzer eine Webseite oder einen Anhang anfordert, für die/den eine Zugangsbeschränkungsrichtlinie gilt, wird der Zugang zu dieser Webseite oder diesem Anhang verweigert, und dem Internetnutzer wird automatisch eine Alarmmeldung als Webseite angezeigt. In seltenen Fällen und wenn ein oder mehrere Elemente der angeforderten Inhalte blockiert sind, ist es unter Umständen nicht möglich, die Alarmmeldungswebseite anzuzeigen, und der Inhalt des angeforderten Elements kann deshalb durch die Warnmeldung ersetzt werden. Jedoch wird der Zugang zur betreffenden Seite weiterhin verweigert.

4.2. Auf den automatischen Alarmmeldungswebseiten gibt es einen Bereich, den Kunden über ClientNet individuell anpassen können.

5. Berichte

5.1. Über ClientNet ist das Resultat der in Ziffer 3.1 beschriebener Richtlinien für die Zugangsbeschränkung verfügbar.

5.2. Um eine Verwaltung nach Usern oder nach Gruppen und ein entsprechendes Berichtswesen zu ermöglichen, muss der Kunde die hierfür erforderliche Softwareanwendung (den "Client Site Proxy") gemäß den Installationsrichtlinien installieren, die mit dem Client Site Proxy ausgeliefert werden. Die Nutzung dieser Software richtet sich nach der End-User-Lizenzvereinbarung, die mit dem Client Site Proxy ausgeliefert wird.

5.3 Der Kunde erkennt an, dass detaillierte ClientNet-Berichterstellungsdaten nur für einen Zeitraum von maximal vierzig (40) Tagen von Symantec gespeichert werden und nach Ablauf dieses Zeitraums nicht mehr für den Kunden verfügbar sind. Zusammenfassende ClientNet-Daten sind für einen Zeitraum von maximal zwölf (12) Monaten verfügbar.

5.4 Der Kunden kann für den detaillierten ClientNet-Bericht einen verlängerten Berichterstellungszeitraum von bis zu sechs (6) Monaten anfordern, indem er WSS Enhanced Data Retention abonniert.

6. Web v2 URL - Sonderbedingungen

6.1. KEINE WEB-FILTER-SOFTWARE KANN EINEN 100%IGEN ERKENNUNGSERFOLG GARANTIEREN. SYMANTEC WIRD SICH JEDOCH BESTMOGLICH BEMUHEN, BLOCKIERTE URLs UND INHALTE AUFZUSPUREN. DER KUNDE NIMMT ZUR KENNTNIS, DASS DIE ERKENNUNG VON DEN VOM KUNDEN AUSGEWAHLTEN EINSTELLUNGSMOGLICHKEITEN, VON DER BEKANNTHEIT NEUER TECHNIKEN UND SONSTIGEN UNWAGBARKEITEN ABHANGEN KANN, WELCHE IN SELTENEN AUSNAHMEFALLEN DIE ERKENNUNG VERHINDERN KONNEN. SYMANTEC KANN GRUNDSATZLICH FUR HIERAUS ENTSTEHENDE SCHADEN ODER VERLUSTE NICHT EINSTEHEN UND HAFTET NUR NACH DEN VORSCHRIFTEN DIESES VERTRAGES.

6.2. Symantec weist ausdrücklich darauf hin, dass die Konfiguration von Web v2 URL ausschließlich der Verantwortung des Kunden unterliegt. Web v2 URL ist nur dazu gedacht, dem Kunden bei der Durchsetzung von Nutzungsbestimmungen („Acceptable Computer Use Policy" oder ein entsprechender Dokumente) zu unterstützen. Die Einwilligung der betroffenen Mitarbeiter des Kunden wird - soweit erforderlich- vom Kunden sichergestellt. Die Verantwortung gegenüber den Nutzern und Betroffenen liegt allein beim Kunden. In manchen Ländern kann die Nutzung von der Zustimmung einzelner Personen abhängen; dem Kunden wird deshalb geraten, vor dem Einsatz von Web v2 URL stets die örtlich geltenden Gesetze zu prüfen. Symantec haftet nicht für die zivil- oder strafrechtlichen Folgen des Betriebs von Web v2 URL für den Kunden.

6.3 Der Web-Datenverkehr (Traffic) des Kunden bei der Nutzung von Web v2 URL darf dreißig Megabyte (30 MB) je Benutzer und Tag nicht überschreiten (berechnet als Durchschnitt pro Nutzer in Bezug auf die gesamte vereinbarte Nutzungsumfang des Kunden für Web v2 URL). Für den Fall, dass dieser Tagesgrenzwert überschritten wird, behält sich Symantec folgende Maßnahmen vor:

6.3.1 Verweigerung der Bereitstellung oder vorübergehende Einstellung von Web v2 URL im Ganzen oder in Teilen mit sofortiger Wirkung bis zum Unterbleiben der übermäßigen Nutzung; oder

6.3.2 Aufforderung der Kunden zum Erwerb eines zusätzlichen Nutzerkontingents entsprechend dem tatsächlichen Web-Datenaufkommen des Kunden und Ausstellung zusätzlicher Rechnungen und/oder Anpassung nachfolgender Rechnungen, sodass die Gebühren für die Erhöhung des angemeldeten Nutzungsaufkommens anteilmäßig für den verbleibenden Teil des laufenden Rechnungszeitraums gedeckt werden.

H Der Symantec MessageLabs Email Archiving.cloud (P) Service

1. Dienst-Übersicht

1.1 Der Symantec MessageLabs Email Archiving.cloud (P) Service, der Symantec MessageLabs Email Archiving.cloud Lite (P) Service und der Symantec MessageLabs Email Archiving.cloud Premium (P) Service (zusammen als „Archivierungsdienst (P)" bezeichnet) sind hybride verwaltete Archivierungsdienste zum Archivieren, Speichern und Abrufen von E-Mails.

1.2 Für Kunden mit *höchstens 500 Benutzern* umfasst der *Symantec MessageLabs Email Archiving.cloud Lite (P) Service* Folgendes:

(i) Standardfunktionen gemäß der Beschreibung in Klausel 3 unten;
(ii) 3-jährige Aufbewahrungszeit;
(iii) Maximaler Speicherplatz von 3GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl).

Für Kunden mit *mehr als 500 Benutzern* umfasst der *Symantec MessageLabs Email Archiving.cloud Lite (P) Service* Folgendes:

(i) Standardfunktionen gemäß der Beschreibung in Klausel 3 unten;
(ii) 3-jährige Aufbewahrungszeit;
(iii) Maximaler Speicherplatz von 1,5 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl).

1.3 Für Kunden mit *höchstens 500 Benutzern* umfasst der *Symantec MessageLabs Email Archiving.cloud (P) Service* Folgendes:

(i) Standardfunktionen gemäß der Beschreibung in Klausel 3 unten;
(ii) 10-jährige Aufbewahrungszeit;
(iii) Maximaler Speicherplatz von 10 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl).

Für Kunden mit *mehr als 500 Benutzern* umfasst der *Symantec MessageLabs Email Archiving.cloud (P) Service* Folgendes:

(i) Standardfunktionen gemäß der Beschreibung in Klausel 3 unten;
(ii) Unbegrenzte Aufbewahrungszeit;
(iii) Maximaler Speicherplatz von 6 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl).

1.4 Für Kunden mit *höchstens 500 Benutzern* umfasst der *Symantec MessageLabs Email Archiving.cloud Premium (P) Service* Folgendes:

(i) Standardfunktionen gemäß der Beschreibung in Klausel 3 unten;
(ii) Premium-Funktionen gemäß der Beschreibung in Klausel 4 unten;
(iii) 10-jährige Aufbewahrungszeit;
(iv) Maximaler Speicherplatz von 10 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl).

Für Kunden mit *mehr als 500 Benutzern* umfasst der *Symantec MessageLabs Email Archiving.cloud Premium (P) Service* Folgendes:

(i) Standardfunktionen gemäß der Beschreibung in Klausel 3 unten;
(ii) Premium-Funktionen gemäß der Beschreibung in Klausel 4 unten;
(iii) Unbegrenzte Aufbewahrungszeit;
(iv) Maximaler Speicherplatz von 6 GB pro Benutzer (berechnet als Durchschnitt pro Benutzer basierend auf der Gesamtbenutzerzahl).

1.5 Der Kunde muss die Journaling-Funktion in Exchange konfigurieren, um eine Kopie interner und externer E-Mails im lokalen Postfach auf dem Exchange-Server abzulegen. Eine Einrichtung bzw. Einrichtungen, die sich hinter der Firewall im Unternehmensnetzwerk des Kunden befindet bzw. befinden („E-Mail-Archivierungseinrichtung/-en") kann bzw. können danach verwendet werden, um Daten aus diesem Postfach zu ziehen, damit sie an den Archivierungsdienst (P) gesendet werden können. E-Mails werden erst im Journaling-Postfach gelöscht, wenn die Speicherung im Archivierungsdienst (P) bestätigt worden ist.

1.6 Symantec überwacht die tatsächliche Nutzung des Archivierungsdienstes (P) durch den Kunden. Wenn die tatsächliche Speicherkapazität die gekaufte Speicherkapazität übersteigt, wird der Kunde aufgefordert einen zusätzlichen Speicherblock zu den jeweils geltenden Preisen von Symantec zu kaufen. Symantec stellt zusätzliche Rechnungen aus und/oder passt spätere Rechnungen entsprechend an, um die Kosten für die Speicherplatzerweiterung anteilig für die Restdauer des Abrechnungszeitraums abzudecken.

1.7 Der Kunde erklärt sich damit einverstanden, dass archivierte E-Mails, erst nach Ablauf der zugewiesensen Aufbewahrungszeit gelöscht werden können. Dies bedeutet, dass es nicht möglich ist, wahlweise einzelne E-Mails zu löschen.

2. Dienstaktivierung

2.1 Der Kunde muss das Symantec-Bereitstellungsformular vollständig ausfüllen.

2.2 Der Kunde muss eine E-Mail-Archivierungseinrichtung bzw. -einrichtungen bestellen, um den Archivierungsdienst (P) zu empfangen. Die bestellte(n) E-Mail-Archivierungsanwendung(en) (sowie die beiliegende Dokumentation) werden zur Installation und Konfiguration an den Kunden gesendet.. Der Kunde ist für alle Versand- und Versicherungskosten sowie Abgaben und Steuern, die hinsichtlich der E-Mail-Archivierungseinrichtung anfallen verantwortlich.

2.3 Symantec setzt sich mit dem Kunden in Verbindung, um einen Termin für ein anfängliches Kundengespräch anzusetzen.

2.4 Der Kunde muss im Kunden-Setup-Dokument aufgeführte Aktionen vor dem anfänglichen Kundengespräch ausführen. Dazu gehören insbesondere folgende Aktionen:

2.4.1 Einrichtung eines neuen Active-Directory-Benutzerkontos;
2.4.2 Einrichtung weiterer Active-Directory-Gruppen;
2.4.3 Hinzufügen von Benutzern zu Exchange-Gruppen;
2.4.4 Firewall-Konfiguration (falls erforderlich);
2.4.5 Aktivierung der Journaling-Funktion in Microsoft Exchange (frühestens 48 Stunden vor der Installation der E-Mail-Archivierungseinrichtung);
2.4.6 Installation der E-Mail-Archivierungseinrichtung (eingebaut und hochgefahren);
2.4.7 Sicherstellung, dass alle zur Archivierung benötigten Postfächer „für E-Mail aktiviert" sind;
2.4.8 Konfiguration des Fernzugriffs für Symantec.

Falls der Kunde beim Kunden-Setup Hilfe benötigt kann er einen Kundendienstmanager von Symantec kontaktieren.

2.5 Das anfängliche Kundengespräch erfolgt über WebEx. Bei diesem Gespräch werden von den Parteien folgende Aktionen durchgeführt:

2.5.1 Überprüfung, dass alle Aktionen gemäß dem Kunden-Setup-Dokument ausgeführt wurden;
2.5.2 Installation der Archivierungs- und sonstiger Software mittels des Symantec-Dokuments über Archivierungsinstallationsverfahren;
2.5.3 Überprüfung der Active-Directory-Einstellungen;
2.5.4 Aktivierung des Dienstes;
2.5.5 Überprüfung der Benutzerschnittstellenverfügbarkeit;

2.5.6 Überprüfung der Archivierung (Site-to-Site);
2.5.7 Erstellung von Verschlüsselungscode-Kopien gemäß dem Symantec-Dokument über Codesicherungsverfahren.
2.6 Eine Schulungssitzung kann beim oder nach dem anfänglichen Kundengespräch in Anspruch genommen werden und umfasst Sitzungen, die sich auf folgende Themen konzentrieren: (i) IT, (ii) Richtlinie, (iii) Überwachung, (iv) Endbenutzer.
2.7 Nach der Überprüfung und ungefähr eine (1) Woche nach der Aktivierung wird ein eintägiges Meeting angesetzt. Danach kann der Kunde für weitere Hilfe die Standard-Supportleistungen in Anspruch nehmen.

3. Standardfunktionen
3.1 *Adressauflösung und Verteilerliste/Gruppenerweiterung.* Alle von Exchange als interne Adressen markierten E-Mail-Adressen werden im entsprechenden Benutzer-Postfach aufgelöst. Für jede Verteilerliste mit einer Referenzierung auf einen Empfänger der Nachricht wird eine Liste mit zu dem Zeitpunkt aktuellen Mitgliedschaftsinformationen in Form zusätzlicher Metadaten zur E-Mail-Nachricht erfasst.
3.2 *Volltextindex*. Die E-Mail-Archivierungseinrichtung kann Textinhalte aus verschiedenen Anhängetypen sowie gemeinsamen Feldern in der Nachricht extrahieren, um die Erstellung eines Volltextindexes zum Suchen im Archivierungsdienst (P) zu unterstützen.
3.3 *Verschlüsselung.* Nachrichteninhaltsdaten und -indexdaten (mit der Ausnahme von Feldern wie Datum und anderen nicht personenbezogenen Informationen) werden unter Anwendung von auf Industriestandards beruhenden Verschlüsselungstechniken und basierend auf einem kundenspezifischen, nur von dem betreffenden Kunden verwendbaren Verschlüsselungscode verschlüsselt. Nur der Kunde hat Zugriff auf alle Passwörter, Verschlüsselungscodes und Konfigurationseinstellungen, und dementsprechend sollte der Kunde sicherstellen, dass diese sicher verwahrt und im Escrow-Verfahren oder an einem anderen geeigneten Ort aufbewahrt werden. Symantec übernimmt keine Haftung für den Verlust von Passwörtern, Verschlüsselungscodes oder Konfigurationseinstellungen. Der Kunde nimmt zur Kenntnis, dass der Verlust von Passwörtern und Verschlüsselungscodes dazu führt, dass auf das Archiv nicht mehr zugegriffen werden kann.
3.4 *Aufbewahrungsrichtlinien*. Der Kunde kann über die Benutzerschnittstelle Aufbewahrungsrichtlinien definieren und aktualisieren. In jeder Aufbewahrungsrichtlinie können bestimmte Kriterien berücksichtigt werden, etwa die beteiligten Parteien, Schlüsselwörter/Schlüsselwendungen im Inhalt sowie die Typen angehängter Dateien. Wenn die jeweiligen Nachrichten archiviert werden, werden sie im Vergleich mit der jeweils aktiven Aufbewahrungsrichtlinienmenge bewertet. Falls eine Nachricht mehr als einer Aufbewahrungsrichtlinie entspricht, wird die Richtlinie mit der längsten Aufbewahrungszeit angewendet. Falls der Nachricht keiner bestimmte Aufbewahrungsrichtlinie entspricht, wird die Standardaufbewahrungsrichtlinie angewendet.
3.5 *InfoTags (Metadaten)*. Der Kunde kann InfoTags über die Benutzerschnittstelle definieren und aktualisieren. In jedem InfoTag können bestimmte Kriterien berücksichtigt werden, etwa die beteiligten Parteien, Schlüsselwörter/Schlüsselwendungen im Inhalt und die Typen angehängter Dateien. Wenn die jeweiligen Nachrichten archiviert werden, werden sie gegenüber der jeweils aktiven Menge von InfoTags bewertet und mit jedem, der anwendbar ist, markiert.
3.6 *Richtlinienverfolgung*. An Aufbewahrungs- und Überwachungsrichtlinien vorgenommene Änderungen werden vom System in einer nicht änderbaren Form zur späteren Bezugnahme geführt. Der Kunde kann von aktuellen oder früheren Richtlinienversionen über die Benutzerschnittstelle Dateien im PDF-Format erstellen.
3.7 *Verfolgung archivierter Benutzer*. Dem System wird jede Nacht eine Liste mit allen Benutzern mit einem Exchange-Postfach unterbreitet, damit eine fortlaufende Liste aller seit der Implementierung des Archivierungsdienstes (P) bestehender Postfächer geführt wird. Diese Informationen können genutzt werden, um Richtlinien und Aufbewahrungsorte für den Vernichtungsstopp aus juristischen Überlegungen („Legal Holds") zu erstellen, um die Benutzer referenzieren, welche im Active Directory gelöscht wurden, sowie um anderen Benutzern Zugang zu den E-Mails ehemaliger Mitarbeiter zu verschaffen.
3.8 *Anhänge-Stubbing*. Der Kunde kann Funktionen aktivieren, die die Inhalte von Anhängen im E-Mail-System des Kunden („Postfachdaten") durch einen Hinweis auf die entsprechende Kopie im Archiv ersetzen. Der Kunde kann Stubbing-Richtlinien mit verschiedenen Regeln für jede Postfachgruppe basierend auf dem Alter und der Größe der Nachricht sowie des Ordners, in dem sie abgelegt ist, definieren und aktualisieren. Um die automatische Wiederherstellung des ursprünglichen Anhangs aus dem Archiv zu ermöglichen, wenn Benutzer E-Mails weiterleiten, kann der Kunde das benutzerdefinierte Formular zum Anhänge-Stubbing in der Organisationsformularbibliothek (einem speziellen öffentlichen Ordner auf dem Exchange-Server) installieren. Outlook installiert anschließend automatisch das benutzerdefinierte Formular vom Server. Um den Zugriff zum Abrufen von Anhängen außerhalb des Netzwerks des Kunden zu ermöglichen, kann der Kunde den Archiv-Proxy auf den Front-End-(OWA-)Exchange-Servern installieren. In der Standardeinstellung werden nur zuvor bereits archivierte Postfachdaten einem Stubbing-Verfahren unterzogen. Der Kunde kann eine Option aktivieren, mit der eine Kopie von Anhängen gespeichert wird, die nicht zuvor archiviert wurden, um zu ermöglichen, dass im Postfach enthaltene Anhänge einem Stubbing-Verfahren unterzogen werden. Um Aufbewahrungszeiten der Anhänge zu definieren, kann der Kunde kann Aufbewahrungsrichtlinien pro Postfach konfigurieren. Falls keine solche Festlegung erfolgt ist, wird die Standardaufbewahrungsrichtlinie auf diese Elemente angewendet. Mittels dieses Vorgangs gespeicherte Anhänge können nicht im Archiv durchsucht werden.
3.9 *Endbenutzerzugriff*. Der Kunde kann einzelnen Benutzern Zugriffsmöglichkeiten zum Zweck der Durchsuchung des Archivs entweder innerhalb der Web-Benutzerschnittstelle oder direkt in Outlook zu verschaffen.
3.10 *Zugriff für Beweissicherung*. Der Kunde kann innerhalb der Benutzerschnittstelle Suchvorgänge im gesamten Archiv durchführen. Der Kunde kann einen Aufbewahrungsort für den Vernichtungsstopp aus juristischen Überlegungen („Legal Hold") einrichten. Dabei handelt es sich um ein Repository für Nachrichten, die für eine bestimmte Angelegenheit relevant sind. Der Kunde kann dieses Repository genauso durchsuchen wie das aktive Archiv.
3.11 *Ad-Hoc-Aufbewahrungsorte für den Vernichtungsstopp aus juristischen Überlegungen („Ad-Hoc Legal Holds").* Der Kunde kann die Richtlinienbenutzerschnittstelle nutzen, um Ad-hoc-Aufbewahrungsorte für den Vernichtungsstopp aus juristischen Überlegungen („Ad-Hoc Legal Holds") zu definieren und aktualisieren. Für jeden „Legal Hold" können bestimmte Kriterien berücksichtigt werden, etwa die beteiligten Parteien, Schlüsselwörter/Schlüsselwendungen im Inhalt und die Typen angehängter Dateien. Wenn die jeweiligen Nachrichten archiviert werden, werden sie gegenüber der jeweils aktiven Menge von „Legal Holds" bewertet. Die Nachricht ist mit jedem „Legal Hold" verknüpft, mit dem sie übereinstimmt. Um vorhandene archivierte Daten an einem „Ad-Hoc Legal Hold" zu erfassen, kann der Kunde eine Suche mit ähnlichen Kriterien durchführen, die Ergebnisse in einen Ordner kopieren und die Inhalte des Ordners anschließend an den „Legal Hold" kopieren. Die Aufbewahrungszeit für jeden „Ad-Hoc Legal Hold" ist unbegrenzt lang. Alle Nachrichten an einem bestimmten „Ad-Hoc Legal Hold" werden aufbewahrt, bis der betreffende „Ad-Hoc Legal Hold" freigegeben wird.
3.12 *Personenbasierte Aufbewahrungsorte für den Vernichtungsstopp aus juristischen Überlegungen („Legal Holds")*. Der Kunde kann die Richtlinienbenutzerschnittstelle nutzen, um personenbasierte „Legal Holds" zu definieren und zu aktualisieren. Jeder personenbasierte „Legal Hold" definiert eine Menge von Benutzern. Sofern eine Nachricht eine der an einem bestimmten Aufbewahrungsort aufgelisteten Personen betrifft, ist die Archivierung mit diesem Aufbewahrungsort verknüpft. Das System erfasst automatisch auch vorhandene, zu den Benutzern gehörende und momentan vom Aufbewahrungsort referenzierte E-Mails und erstellt eine neue Kopie der Nachrichten an dem Aufbewahrungsort. Immer wenn Benutzer aus der Definition eines personenbezogenen „Legal Hold" entfernt werden, werden Nachrichten, die nur zu diesem Benutzern gehören, automatisch von diesem Aufbewahrungsort entfernt.

Nachrichten für momentan aufgelistete Benutzer, die von einem Aufbewahrungsort erfasst sind, werden aufbewahrt, bis der betreffende Aufbewahrungsort freigegeben wird.
3.13 *Datenexport*. Nachrichten können aus dem aktiven Archiv oder vom Aufbewahrungsort für den Vernichtungsstopp aus juristischen Überlegungen („Legal Hold") in PST-Dateien exportiert werden. Das System erstellt wegen Dateigrößebeschränkungen, falls nötig, mehrere PST-Dateien.
3.14 *Berichterstattung*. Berichte zur Größe und Vergrößerung des Archivs stehen dem Kunden innerhalb der Benutzerschnittstelle zur Verfügung und können im HTML-Format angezeigt oder in eine PDF- oder CSV-Datei (nur Daten) exportiert werden.
3.15 *Audit Trail*. Such-, Nachrichtenanzeige-, Export-, Abruf- und Überwachungsaktivitäten werden verfolgt. Der Audit Trail kann als Eigenschaft einer bestimmten Nachricht angesehen werden. Ein Audit Trail Viewer für alle Nachrichten ermöglicht gefilterte Ansichten abhängig von der Art der Aktivität, der Person, welche die Aktivität durchgeführt hat, und/oder dem Datum der Aktivität.
3.16 *Active-Directory-Integration.* Der Zugriff auf das Archiv wird verwaltet, indem Benutzer (oder vorhandene Benutzergruppen) einer Menge vordefinierter Sicherheitsgruppen in Active Directory hinzugefügt werden. Jeder dieser Gruppen ist eine Menge von Berechtigungen zugeordnet. Benutzer können aufgrund ihrer Mitgliedschaft in mehreren dieser Sicherheitsgruppen diverse Funktionen ausüben. Die Authentifizierung erfolgt direkt gegenüber Active Directory. Die Benutzer melden sich mittels ihrer Active-Directory-Benutzernamen und -Passwörter an, und Benutzer mit deaktivierten Konten verlieren ihre Archivzugangsrechte. Active-Directory-Gruppen können zum Zweck einer vereinfachten Verwaltung von Elementen wie Richtlinien auch über verschiedene andere Aspekte des Systems referenziert werden. Gruppenmitgliedschaftsänderungen werden mittels eines jede Nacht durchgeführten Synchronisierungsprozesses erfasst.
3.17 *Aufbewahrungs- und Entsorgungsverwaltung.*
Ausgehend von den vom Kunden innerhalb der Benutzerschnittstelle definierten Aufbewahrungsrichtlinien werden vom Archivierungsdienst (P) Nachrichten kategorisiert. Ferner wird entweder ein Entsorgungszieldatum zugewiesen oder der Monat aufgezeichnet, in dem die Nachricht archiviert wurde, um unbegrenzt lange aufbewahrt zu werden. Die Entsorgungszieldaten werden am jeweiligen Monatsbeginn ausgerichtet. Sobald Nachrichten das für sie vorgegebene Entsorgungszieldatum erreicht haben, kann bzw. können der bzw. die berechtigte(n) Benutzer des Kunden die Entsorgung für alle Nachrichten formal bewilligen, die diesem Entsorgungszieldatum zugeordnet sind. Hinsichtlich Nachrichten, die mit Blick auf eine unbegrenzt lange Aufbewahrungszeit archiviert werden, kann bzw. können der bzw. die berechtigte(n) Benutzer des Kunden die Entsorgung für alle Nachrichten formal bewilligen, die in einem bestimmten Monat archiviert wurden. Der Kunde akzeptiert und bestätigt, dass für eine Entsorgung vorgesehene Daten von Speichermedien jeglicher Art (insbesondere Sicherungen) nicht so wiederhergestellt werden können, dass sie visuell lesbar sind.

4. Premium-Funktionen
Folgende Funktionen stehen nur für den *Symantec MessageLabs Email Archiving.cloud Premium (P) Service* zur Verfügung:
4.1 *Überwachung.*
4.1.1 *Automatische Auswahl für aufsichtliche Überprüfung.* Der Kunde kann über die Benutzerschnittstelle Richtlinien definieren und aktualisieren, mittels welcher einer Überprüfungswarteschlange Nachrichten hinzugefügt werden. In jeder Richtlinie können die beteiligten Parteien, Schlüsselwörter/Schlüsselwendungen im Inhalt und Dateitypen berücksichtigt werden. Ferner können Stichprobenrichtlinien für bestimmte Benutzer konfiguriert werden.
4.1.2 Aufsichtliche Überprüfung. Der Kunde kann Zugriffsrechte für Überprüfer zuweisen, die Nachrichten lesen sollen, welche der Überprüfungswarteschlange hinzugefügt wurden, und kann sie als akzeptabel markieren oder nicht.
4.2 *Bloomberg-Archivierung*
4.2.1 Der Symantec MessageLabs Email Archiving.cloud Premium (P) Service nutzt Protokollierungsfunktionen des Bloomberg Professional Service, der E-Mail- und Sofortnachrichtengespräche in XML-Dateien aufzeichnet, welche jede Nacht auf die FTP-Site von Bloomberg gestellt werden.
4.2.2 Wenn der Kunde den Bloomberg Professional Service abonniert, kann die E-Mail-Archivierungseinrichtung genutzt werden, um eine Kopie dieser XML-Dateien von der FTP-Site zur Umwandlung in Nachrichten im HTML-Format und zur Versendung an das Archiv abzurufen.
4.2.3 Das FIRM-Format wird unterstützt, nicht jedoch das ACCOUNT-Format oder das ursprüngliche Extraktionsformat von Bloomberg-Protokollen.
4.2.4 Im Zuge der Bloomberg-Archivierungsintegration wird kein Inhalt auf der FTP-Site von Bloomberg gelöscht. Es wird dabei jedoch verfolgt, welche Dateien verarbeitet wurden. Da über Bloomberg regelmäßig Inhalte von der FTP-Site entfernt und beim Bloomberg-Archivierungsintegrationsprozess Kopien gelöscht werden, die von Bloomberg in den E-Mail-Archivierungseinrichtungen erstellt wurden, muss der Kunde überwachen, ob die Archivierungsintegration ständig betrieben werden kann, so dass Dateien, bevor sie mittels der Bloomberg-Archivierungsintegration abgerufen und vollständig verarbeitet werden können, nicht gelöscht werden.
4.2.5 Um zu identifizieren, welche in der Extensible Markup Language (XML) referenzierten Benutzer interne Mitarbeiter sind, wird eine Liste mit Bloomberg-FIRM-Kennzeichnern verwendet. Die Bloomberg-Archivierungsintegration sieht eine webbasierte Abbildungsbenutzerschnittstelle vor, welche ermöglicht, dass ein Administrator die Bloomberg-Benutzerkonten jeweils den entsprechenden Active-Directory-Benutzerkonten zuordnet. Wenn die XML-Dateien verarbeitet werden, wenn eine Nachricht einen internen Benutzer referenziert, der noch nicht abgebildet wurde, wird die Adresse der nicht abgebildeten Adressliste hinzugefügt und die Nachricht nicht verarbeitet. Sobald der Administrator diese Adressen abgebildet hat, können sie die erneute Verarbeitung der verknüpften Nachrichten auslösen. Die aufgelösten E-Mail-Unternehmensadressen werden als Adressen der Absender/Empfänger der Nachricht verwendet.
4.2.6 Ein Informationsblock im Nachrichtenhauptteil liefert zusätzliche Informationen zu den tatsächlichen Adressen/Anzeigenamen der Nachrichten-/Gesprächsparteien, darunter Bloomberg-Kontoinformationen des betreffenden Benutzers.

5. Altdatenimport
5.1 Vorbehaltlich der Entrichtung einer Gebühr basierend auf der Menge der zu importierenden Daten kann der Kunde Altdaten in den Archivierungsdienst (P) importieren. Für den Fall, dass die tatsächliche Menge Altdaten die Menge der erworbenen Importdaten übersteigt, behält Symantec sich das Recht vor, die für diese zusätzlichen Daten entstehenden Kosten zu den jeweiligen Standardpreisen in Rechnung zu stellen.
5.2 Entscheidet sich der der Kunde zur Erleichterung des Datenimports unabhängige Software von Dritten zu nutzenakzeptiert der Kunde, dass Symantec für derartige Software von Dritten keine Verantwortung übernimmt und dass der Kunde auf eigenes Risiko und eigene Kosten derart verfährt.

6. Dienstkündigung
6.1 Bei Ablauf/Kündigung des Archivierungsdienst (P) löscht Symantec die Daten des Kunden aus dem Archiv. Vor dem Ablauf kann der Kunde seine Daten aus dem Archiv extrahieren, oder der Kunde kann anfordern, dass der von Symantec ernannte externe Partner die archivierten Daten im PST-Dateiformat gemäß den nachfolgend in Klausel 6.2 beschriebenen Bestimmungen an den Kunden zurücküberträgt.

6.2 Falls der Kunde eine Übertragung der archivierten Daten bei Ablauf durch den von Symantec ernannten externen Partner anfordert, gilt Folgendes:
6.2.1 Der Kunde muss eine Vereinbarung direkt mit dem ernannten externen Partner abschließen. Symantec ist kein Vertragspartner in einer solchen Vereinbarung.
6.2.2 Da die Daten in einem verschlüsselten Format gespeichert sind, muss der Kunde dem externen Partner einen Verschlüsselungsschlüssel bereitstellen, um die E-Mails in ein unverschlüsseltes Format zu dekodieren.
6.2.3 Der Kunde trägt die Kosten der Übertragung. Die Kosten werden in der Vereinbarung mit dem externen Partner vereinbart. Die Höhe der Kosten hängt von folgenden Faktoren ab: (i) Datenmenge; (ii) Format/Medium der Übertragung; (iii) Kosten für die Einrichtung des Übertragungsprozesses; (iv) Zeit- und Materialaufwand für die Durchführung der Übertragung.
6.2.4 Symantec behält sich das Recht vor, seine zu diesem Zeitpunkt geltenden Gebühren für die Speicherung in Rechnung zu stellen, falls die Daten zum Datum des Inkrafttretens des Ablaufs nicht exportiert und gelöscht wurden.

7. Dienst-Geschäftsbedingungen
7.1 Symantec ist berechtigt, den Archivierungsdienst (P) nach billigem Ermessen ohne Vorankündigung umgehend zu kündigen und jegliche von Symantec als notwendig erachtete Abwehrmaßnahmen zu ergreifen:
7.1.1 Im Fall einer Anweisung durch ein Gericht oder eine zuständige Behörde;
7.1.2 Im Fall eines Angriffs auf den Archivierungsdienst (P) oder das Netzwerk;
7.1.3 Im Fall, dass der Kunde oder seine Benutzer gegen die Richtlinie über akzeptable Nutzung gemäß Klausel 7.3 unten verstoßen.
7.2. Der Kunde ist stellt sicher, dass er sowie alle seine Benutzer die Richtlinie über akzeptable Nutzung gemäß Klausel 7.3 unten kennen und erfüllen.
7.3 *Richtlinie über akzeptable Nutzung*. Die Benutzer dürfen unter keinen Umständen twedervorsätzlich, fahrlässig oder schuldlos Handlungen begehen bzw. versuchen oder Beihilfe leisten, die eine Bedrohung des Archivierungsdienstes (P) bewirken können. Zu solchen Handlungen zählen:
7.3.1 Jegliche Versuche, einen Dienst-Host oder ein Netzwerk zum Absturz zu bringen;
7.3.2 „Denial-of-service"-Angriffe oder "Flooding"-Angriffe auf einen Dienst-Host oder ein Netzwerk;
7.3.3 Jegliche Versuche der Umgehung der Benutzer-Authentifizierung oder Sicherheit eines Dienst-Hosts oder Netzwerks;
7.3.4 Jegliche verschwenderische Nutzungen des Archivierungsdienstes (P);
7.3.5 Die Erstellung, Übermittlung, Speicherung oder Veröffentlichung von Viren, schädigenden Programmen oder beschädigten Daten jeglicher Art;
7.3.6 Jegliche sonstigen Handlungen, die sich ungünstig auf den Archivierungsdienst (P) oder dessen Betrieb auswirken können.
7.4 Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrentsprechender Anfertigung von Sicherungskopien eingetreten wäre.
7.5 Der Kunde erkennt an, dass E-Mails personenbezogene Informationen enthalten können und die Archivierung von E-Mails deshalb einer Verarbeitung personenbezogener Daten gleichkommen kann. Der Kunde erkennt ferner an, dass der Archivierungsdienst (P) ein konfigurierbarer Dienst ist und der Kunde für die Konfiguration des Archivierungsdienstes (P) gemäß der Richtlinie über akzeptable Computernutzung des Kunden (bzw. einer entsprechenden Vorgabe) sowie jeglichen anwendbaren Gesetzen oder Verordnungen allein verantwortlich ist. Alle von Symantec zur Verfügung gestellten Vorlagen erfüllen nur die Funktion von Richtvorlagen, anhand derer der Kunde seine eigenen, individuell angepassten Richtlinien und andere Vorlagen erstellen kann. Folglich empfiehlt Symantec dem Kunden, vor der Nutzung des Archivierungsdienstes (P) stets die vor Ort geltenden Gesetze zu prüfen und sicherzustellen, dass er und alle seine Mitarbeiter die Pflichten kennen und erfüllen, die sie hinsichtlich Datenschutzgesetzen und/oder -verordnungen deshalb haben, weil der Kunde den Archivierungsdienst (P) nutzt. In bestimmten Ländern ist es unter Umständen notwendig, vor der Nutzung des Archivierungsdienstes (P) die Zustimmung einzelner Angestellter einzuholen. Symantec übernimmt keine Haftung für eine zivil- oder strafrechtliche Haftung des Kunden, die sich ergeben kann, wenn der Kunde den Archivierungsdienst (P) nutzt. Der Kunde sollte dies bei der Konfiguration des Archivierungsdienstes (P) berücksichtigen.
7.6 Der Kunde muss den Ort des Archivierungsdatenzentrums bei der Bestellung auswählen, und die Gebühren werden basierend auf dieser Auswahl berechnet. WIRD EIN ARCHIVIERUNGSDATENZENTRUM IN DEN VEREINIGTEN STAATEN VON AMERIKA AUSGEWÄHLT, VERPFLICHTET DER KUNDE SICH, ALLE NOTWENDIGEN MASSNAHMEN ZU ERGREIFEN, UM (I) SEINE MITARBEITER, VERTRETER UND AUFTRAGNEHMER SOWIE DRITTE, DIE DAS ZUM ARCHIVIERUNGSDIENST (P) GEHÖRENDE KOMMUNIKATIONSSYSTEM NUTZEN, DARÜBER ZU INFORMIEREN, DASS JEGLICHE INFORMATIONEN, INSBESONDERE PERSONENBEZOGENE INFORMATIONEN ZU EINZELNEN PERSONEN, IN DEN VEREINIGTEN STAATEN VON AMERIKA VERARBEITET WERDEN KÖNNEN; UND (II) DIE ZUSTIMMUNG DIESER MITARBEITER, VERTRETER, AUFTRAGNEHMER UND DRITTEN ZU EINER SOLCHEN VERARBEITUNG EINZUHOLEN, BEVOR DER KUNDE DEN ARCHIVIERUNGSDIENST (P) AUSFÜHRT.
7.7 Der Kunde bestätigt und stimmt darin überein, dass (i) die Symantec-Scandienste (Email AV, Email AS, Email IC und Email CC) nicht alle E-Mails scannen, die ursprünglich im Archiv eingehen, und (ii) die Symantec-Scandienste (Email AV, Email AS, Email IC und Email CC) keine E-Mails scannen, die aus dem Archiv für eine Wiederherstellung in den Benutzer-Postfächern freigegeben werden. Folglich übernimmt Symantec keine Haftung für Viren, Spam, Bilder oder unangemessene Inhalte, die derartige wiederhergestellte E-Mails enthalten könnten.

8. Softwarelizenz
8.1 Die folgenden Geschäftsbedingungen gelten für die auf der Archivierungseinrichtung installierte Software (die "Software"):
8.1.1 Der Kunde bestätigt und akzeptiert, dass Symantec gemäß der Beziehung zwischen dem Kunden und Symantec, Symantec und/oder dessen Zulieferern zu jedem Zeitpunkt der Eigentümer der Software ist. Der vorliegende Vertrag gewährt dem Kunden eine einfache begrenzte Lizenz zur Nutzung der Software in Verbindung mit dem in diesem Anhang beschriebenen Archivierungsdienst und umfasst nicht den Verkauf der Software oder anderer Rechte auf geistiges Eigentum. Symantec und ihre Zulieferer behalten sich sämtliche nicht ausdrücklich nach dem vorliegenden Vertrag eingeräumten Rechte vor.
8.1.2 Der Kunde darf eine Kopie der Software mit einer Archivierungseinrichtung nutzen. Für die Zwecke des vorliegenden Vertrags bedeutet "Nutzung" die Ausführung, Bedienung, Anzeige und Speicherung der Software während der Dauer der Bereitstellung des Archivierungsdienstes für den Kunden.
8.1.3 Die Software ist durch kanadische und US-amerikanische Urheberrechtsgesetze und internationale Abkommen geschützt. Der Kunde darf die Software weder vermieten oder ausleihen noch Kopien der die Software begleitenden Dokumentation anfertigen. Dem Kunden ist nicht gestattet, die Software zu kopieren, zurückzuentwickeln, zu demontieren, dekompilieren, entschlüsseln oder zu versuchen, den Quellcode der Software zu erstellen.
8.1.4 Der Kunde akzeptiert, dass ein Verstoß gegen diese Bestimmungen zu nicht wieder gutzumachendem Schaden für Symantec und seine Zulieferer führt, und willigt hiermit ein, dass Symantec und/oder dessen Zulieferer diesen Abschnitt insbesondere über Leistung des vertraglich Geschuldeten oder Rechtsschutz durch einstweilige Verfügung neben jeglichem weiteren Rechtsschutz, auf den diese Partei andernfalls nach dem Common Law oder Equity-Recht Anspruch hat, geltend machen können.

8.1.5 Sämtliche Technologien, Software, Dokumentationen und Verfahren, die Symantec zur Erbringung des Archivierungsdienstes anwendet, stellen das alleinige Eigentum von Symantec oder seiner Zulieferer dar.

I Der Symantec MessageLabs EIM.cloud Service

1. Dienstbeschreibung

1.1 Der Symantec MessageLabs EIM.cloud Service, im nachfolgenden “EIM”, ist ein Instant-Messaging-Dienst, der die administrative Kontrolle, zentralisierte Speicherung und das Domainverwaltung von SofortNachrichten (Instant Messages) ermöglicht.

1.2 Mit Ausnahme der MSI- und Java-Versionen wird der EIM-Client (“POD”) auf der Workstation jedes Nutzers installiert. Alle Instanzen ermöglichen es dem Nutzer, eine sichere Verbindung zur EIM-Plattform herzustellen und EIM zu nutzen. Der POD hat die folgenden Funktionen:

(a) File sharing;
(b) sichere Konferenzen über Instant Messaging;
(c) Interoperabilität mit öffentlichen Instant-Messaging-Netzwerken (nur mit dem CONNECT-Paket).

1.3 Das EIM-Administration-Tool, eine webbasierte Konsole, ermöglicht es den Administratoren, ihre Domainstruktur und Nutzerbasis zu verwalten.

2. Dienstmerkmale von EIM

Dienstmerkmale – Symantec MessageLabs EIM Communicate.cloud („COMMUNICATE“)

(i) Integriertes File Sharing (100 MB Kapazität pro Nutzer);
(ii) Backup-Lösung auf dem Desktop;
(iii) Möglichkeit, Informationen mit EIM-Nutzern zu teilen, die online oder offline sind;
(iv) Zugangskontrolllisten;
(v) Sichere, 168-bit 3DES SSL verschlüsselte POD-to-POD Kommunikation;
(vi) webbasierte Administrationskonsole;
(vii) umfassende Optionen für die Nutzer-Schnittstelle;
(viii) erweiterte Echtzeiterkennung und -verfolgung;
(ix) Unterstützung einer großen Vielfalt von Proxy-Servern;
(x) HTTP-Tunnelling-Fähigkeiten;
(xi) Alarmmeldungen bei neuen Dateien;
(xii) objektorientiertes Dateisystem mit umfangreichen Suchmöglichkeiten.

Dienstmerkmale – Symantec MessageLabs EIM Connect.cloud („CONNECT“)

Alle Merkmale des COMMUNICATE-Pakets und zusätzlich die folgenden:

(i) Interoperable Instant-Messaging-Übermittlung (AOL, MSN, Yahoo!), gemäß §6;
(ii) SMS-Nachrichten (2 Nachrichten pro Nutzer, oder “Nutzer-Quoten”);
(iii) Protokoll-Möglichkeiten für Instant Messaging.

Dienstmerkmale– COLLABORATE

Alle Merkmale des CONNECT-Pakets und zusätzlich die folgenden:

(i) Integration mit WebEx;
(ii) Integration mit Salesforce.com.

3. Verantwortlichkeit für Account-Nummern und Passwörter

3.1 Der Kunde ist für alle - autorisierten oder unautorisierten - Nutzungen der Administrations-Webseiten ebenso verantwortlich, wie für die Geheimhaltung der Zugangsdaten und der Passwörter. Der Kunde verpflichtet sich, Symantec jede unautorisierte Nutzung des Kunden-Accounts unverzüglich anzuzeigen.

4. Verantwortung für den Inhalt von Nachrichten des Kundenkontos

4.1 Soweit in diesem Vertrag nicht ausdrücklich anders geregelt, gibt Symantec in Bezug auf die Bereitstellung des EIM-Dienstes keine ausdrücklichen oder stillschweigenden Garantien ab. Die Software von Symantec kann insbesondere keinen 100%igen Erkennungserfolg im Hinblick auf Viren und böswilligen Programmcode sicherstellen. Symantec garantiert insbesondere keine 100%ige Virus- oder Spam-Erkennungsrate und lehnt deshalb jede Haftung für Schäden oder Verluste ab, welche sich direkt oder indirekt daraus ergeben, dass EIM SofortNachrichten überhaupt nicht oder fälschlicherweise als Virusträger oder Spam-Mails identifiziert werden, es dann aber nicht sind.

4.2 Symantec gibt keine ausdrücklichen oder stillschweigenden Garantien in Bezug auf die Verfügbarkeit von EIM oder die Fähigkeit von EIM, alle Daten zu erhalten.

4.3 Symantec unterstreicht, dass die Konfiguration von EIM vollständig der Kontrolle des Kunden unterliegt. Die Einwilligung der betroffenen Mitarbeiter des Kunden wird - soweit erforderlich- vom Kunden sichergestellt. Die Verantwortung gegenüber den Nutzern und Betroffenen liegt allein beim Kunden. In manchen Ländern kann die Nutzung von der Zustimmung einzelner Personen abhängen; dem Kunden wird deshalb geraten, vor dem Einsatz von EIM stets die örtlich geltenden Gesetze zu prüfen.

5. Pflichten des Kunden

5.1. Der Kunde verpflichtet sich:

5.1.1 keine Daten, Texte, Videos, Audios, Software oder Inhalte über den POD oder EIM zu übertragen oder zu speichern, die inhaltlich oder deren Übertragung illegal sind;

5.1.2 keine Inhalte über den POD oder EIM zu übertragen oder zu speichern, welche Patente, Marken, Copyrights, Publizitätsrechte oder sonstige geistige Eigentumsrechte verletzen;

5.1.3 keine Inhalte zu übertragen oder zu speichern, welche lokale, regionale, nationale oder internationale Gesetze verletzen, die eine zivil- oder strafrechtliche Haftung begründen;

5.1.4 keine unangeforderten, verkaufsfördernden Inhalte, Werbematerialien, Spams, Spam für IM, Kettenbriefe oder sonstige belästigende Nachrichten zu übertragen;

5.1.5 den POD oder EIM nicht zur öffentlichen Übertragung oder Vorführung von hierzu nicht autorisierten Inhalten zu nutzen;

5.1.6 den POD oder EIM nicht für die absichtliche Übertragung von Inhalten zu nutzen, welche Viren, Würmer, sog. Cancelbots, Zeitbomben, Trojanische Pferde, "Schnüffler", oder sonstige Programme enthalten, die zum Ausspionieren von Informationen anderer Nutzer oder zur Unterbrechung der Funktion oder Verfügbarkeit von Computerprogrammen, Datenbanken, EIMs oder sonstiger Internet-Hosts bestimmt sind; oder

5.1.7 die Identität des POD-Nutzers nicht durch Täuschung (spoofing), Fälschung von Kopfzeilen, die

Verwendung von Drittrelais oder die Herkunft des übertragenen Inhalts auf andere Weise zu verschleiern, einschließlich der Nachahmung einer anderen natürlichen oder juristischen Person.

6. Interoperabilität

6.1 Dem Kunden wird - soweit beauftragt - die Interoperabilitäts-Funktion gemäß vorstehendem § 2 (siehe CONNECT-Paket) zur Verfügung gestellt. Die Interoperabilität mit anderen Instant-Messaging-Providern, einschließlich jedoch nicht beschränkt auf AOL, MSN und Yahoo!, stellt hierbei lediglich eine freiwillige Funktionalität dar, welche vertraglich nicht geschuldet ist. Symantec wird sich bemühen, die Interoperabilität aufrecht zu erhalten und ggf. auszubauen, behält sich jedoch vor, die Interoperabilität im Einzelfall oder insgesamt einzustellen.

7. Datenspeicherung in den USA

7.1 SYMANTEC WEIST DARAUF HIN, DASS SÄMTLICHE NACHRICHTEN AUS TECHNISCHEN GRÜNDEN IN DEN VEREINIGTEN STAATEN GESPEICHERT WERDEN UND DASS NICHT SYMANTEC, SONDERN DER KUNDE FÜR DIE EINHALTUNG DER NATIONALEN INSBESONDERE DER DATENSCHUTZRECHTLICHEN BESTIMMUNGEN VERANTWORTLICH IST. DER KUNDE AKZEPTIERT, DASS DIE KONFIGURATION UND NUTZUNG VON EIM VOLLSTÄNDIG SEINER KONTROLLE UND SEINEM ERMESSEN UNTERLIEGT. Symantec lehnt jede zivil- oder strafrechtliche Haftung ab, die dem Kunden aufgrund des Betriebs von EIM entsteht. Der Kunde sollte dies bei der Konfiguration von EIM berücksichtigen.

8. Protokollierung und Richtlinieneinhaltung

8.1 Der Kunde hat die Möglichkeit, Instant Messages, die über den EIM-Service laufen, zu protokollieren. Dieser Service wird vorbehaltlich der Zahlung der entsprechenden Gebühren für die Protokollierungsfunktionalität bereitgestellt.

8.2 Protokolldateien werden von Symantec täglich an den Kunden weitergeleitet, so dass der Kunde diese Protokolle auf Wunsch in einem kompatiblen Archiv speichern kann.

8.3 Symantec bewahrt Protokolle für einen Zeitraum von drei (3) Jahren auf. Nach Ablauf dieser Frist werden die Protokolle dauerhaft gelöscht. Der autorisierte Vertreter des Kunden kann jederzeit vor Ablauf der vorgenannten dreijährigen (3) Aufbewahrungsfrist auf schriftliche Anfrage (i) eine Kopie dieser Protokolle anfordern oder verlangen, (ii) dass die Protokolle gelöscht werden.

8.4 Der Kunde sollte berücksichtigen, dass er die Protokollierung über die Verwaltungskonsole jederzeit für bestimmte Gruppen oder Teilgruppen deaktivieren kann und die Protokolle deshalb möglicherweise keinen vollständigen Datensatz der Nutzung des EIM-Service durch den Kunden liefern.

8.5 Symantec kann nach einer mindestens sechs (6) Monate zuvor erfolgten schriftlichen Ankündigung die Bereitstellung und Unterstützung des EIM-Service einstellen. Nach Ablauf dieser schriftlichen Benachrichtigungsfrist endet der EIM-Service automatisch.

8.6 Nach Kündigung des EIM-Service kann der Kunde die Aushändigung oder Löschung seiner Protokolle anfordern. Wenn der Kunde es versäumt, innerhalb von neunzig (90) Tagen nach Inkrafttreten der Kündigung sich für eine der beiden Optionen zu entscheiden, werden die Protokolle dauerhaft gelöscht.

8.7 Der Kunde bestätigt und stimmt zu, dass Symantec unter keinen Umständen die Funktion eines Drittanbieter-Downloaders im Sinne der SEC-Bestimmungen übernehmen kann.

9. Softwarelizenz

9.1 Lizenzgewährung

Vorbehaltlich der Bedingungen dieses Vertrags gewährt Symantec dem Kunden das nicht ausschließliche, nicht übertragbare Recht zur Installation und Nutzung der Software für den EIM-Service unter Beschränkung auf die eigenen internen Geschäftsvorgänge des Kunden („Software“ bezeichnet jedes Softwareprogramm von Symantec für den EIM-Service im Objektcode-Format, das von Symantec lizenziert wird und das den Bedingungen des Vertrags unterliegt, insbesondere neue Versionen oder Aktualisierungen, die im Rahmen dieses Vertrages bereitgestellt werden). Alle geistigen Eigentumsrechte an der Software sind und bleiben Eigentum von Symantec (und/oder von deren Zulieferern). Der Software wird von Symantec lizenziert und nicht verkauft. Der Kunde erkennt an, dass die Software und alle damit in Zusammenhang stehenden Informationen, insbesondere Aktualisierungen, Eigentum von Symantec und von deren Zulieferern sind. Der Kunde ist für die Einhaltung der Bedingungen dieses Vertrags oder für deren Verletzung durch jeden einzelnen Endbenutzer verantwortlich und uneingeschränkt haftbar. Der Kunde setzt Symantec unverzüglich von einer unbefugten Nutzung oder von einer Verletzung der Bedingungen dieser Lizenz in Kenntnis.

9.2. Einschränkungen hinsichtlich des Kopierens und der Nutzung

Der Kunde kann die Software unter den folgenden Bedingungen herunterladen und installieren:

9.2.1. Der Kunde darf die Software nicht für mehr als die Anzahl von durch den Kunden lizenzierten Endbenutzerlizenzen herunterladen oder installieren („Endbenutzer“ bezeichnet den physischen Computer, auf dem die Software installiert ist).

9.2.2. Der Kunde darf die Software, soweit dies billigerweise erforderlich ist, für Zwecke der Datensicherung, der Archivierung oder der Wiederherstellung im Notfall kopieren. Eine gedruckte Dokumentation darf vom Kunden nur für den internen Gebrauch vervielfältigt werden („Dokumentation“ bezeichnet in der heruntergeladenen Software enthaltene Benutzerhandbücher und/oder Handbücher zur Bedienung der Software von Symantec.).

9.2.3 Dem Kunden wie auch mit dessen Billigung handelnden Dritten ist es untersagt: (i) die Software ohne vorherige schriftliche Genehmigung von Symantec zu dekompilieren, zu disassemblieren oder rückzuentwickeln, soweit dies nicht nach geltendem Recht ausdrücklich zulässig ist; (ii) Produktkennzeichnungen oder Hinweise auf Eigentumsrechte zu entfernen; (iii) die Software zu vermieten, zu verleihen oder zu Timesharing- oder Servicebüro-Zwecken zu nutzen; (iv) die Software zu verändern, zu übersetzen, anzupassen oder Bearbeitungen davon zu erstellen oder (v) die Software in anderer Weise zu nutzen oder zu kopieren, soweit dies hier nicht ausdrücklich vorgesehen ist.

9.3. Übertragung von Rechten

Der Kunde darf die Softwarelizenz aus diesem Vertrag ohne vorherige schriftliche Zustimmung von Symantec nicht übertragen, abtreten oder weitergeben. Jegliche Übertragung, Abtretung oder Weitergabe entgegen dieser Bestimmung ist nichtig.

9.4. Beschränkte Gewährleistung und Haftungsausschluss

9.4.1 Symantec gewährleistet, dass nach dem Herunterladen die Software in allen wesentlichen Gesichtspunkten der aktuellen Dokumentation von Symantec entspricht.

9.4.2 Die vorstehende Gewährleistung gilt nicht, wenn: (i) die Software nicht gemäß diesem Vertrag oder der Dokumentation genutzt wird; (ii) die Software oder Teile davon durch einen anderen Rechtsträger als durch Symantec verändert wurden oder (iii) eine Fehlfunktion in der Software durch Anlagen oder Geräte des Kunden oder durch fremde Software verursacht wurde.

9.4.3 DIE HAFTUNG VON SYMANTEC FÜR VERLETZUNGEN DER OBIGEN GEWÄHRLEISTUNG BESCHRÄNKT SICH EINZIG UND AUSSCHLIESSLICH AUF DEN ERSATZ DER SOFTWARE, SOWEIT EIN ERSATZ VERFÜGBAR IST.

SYMANTEC GEWÄHRLEISTET NICHT, DASS DER BETRIEB DER SOFTWARE EIN UNUNTERBROCHENER ODER FEHLERFREIER IST. SYMANTEC SCHLIESST AUSDRÜCKLICH VERTRAGLICHE, KONKLUDENTE UND SONSTIGE GEWÄHRLEISTUNGEN JEDER ART AUS, INSBESONDERE GEWÄHRLEISTUNGEN EINER DURCHSCHNITTSQUALITÄT, EINER ZUFRIEDENSTELLENDEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

9.5. Kündigung

Mit Kündigung des EIM-Service oder des Vertrags enden mit sofortiger Wirkung alle hier gewährten Rechte des Kunden zur Nutzung der Software; der Kunde muss alle Kopien der Software und der Dokumentation umgehend an Symantec zurückgeben oder vernichten.

J – Der Symantec MessageLabs Policy Based Encryption.cloud Service

1. Dienstbeschreibung

1.1 Der Symantec MessageLabs Policy Based Encryption.cloud Service („PBE") bietet die Möglichkeit zum Senden und Empfangen verschlüsselter E-Mails basierend auf der E-Mail-Sicherheitsrichtlinie des Kunden.

1.2 Um PBE beziehen zu können, muss der Kunde auch folgende Dienste abonnieren:

- **Symantec MessageLabs Email Boundary Encryption.cloud („BE")** gemäß der Beschreibung in Anhang 2 Anlage E; und
- **Symantec MessageLabs Email Content Control.cloud („Content Control" oder „Email CC")** gemäß der Beschreibung in Anhang 2 Anlage D.

1.3 PBE bietet folgende Funktionalität:

- Möglichkeit der Nutzung von Email CC zum Definieren von Richtlinien für die Verschlüsselung ausgehender E-Mails;
- Zustellung verschlüsselter E-Mails in den Posteingang eines externen Empfängers;
- Empfänger erhält über ein sicheres Web-Portal Zugriff auf die verschlüsselte E-Mail;
- Empfänger kann auf das sichere Web-Portal zugreifen, um auf die E-Mail in einem verschlüsselten Format zu antworten.

2. PBE-Funktionen

2.1 PBE ermöglicht dem Kunden das Senden verschlüsselter E-Mails, die direkt in den Posteingang eines Empfängers zugestellt werden, ohne dass der Empfänger dafür Software herunterladen muss.

2.2 Der Kunde kann als Verschlüsselungsmethode entweder Push oder Pull konfigurieren. Für Symantec MessageLabs Policy Based Encryption.cloud (Z) ("PBE Z") wird durch die Email CC-Regel festgelegt, ob Push oder Pull konfiguriert wird. Für Symantec MessageLabs Policy Based Encryption.cloud (E) ("PBE E") ist die standardmäßige Verschlüsselungsmethode Pull, die jedoch durch den Empfänger in Push geändert werden kann, wozu im Secure-Web-Portal des Empfängers die Secure Reader-Funktion heruntergeladen werden muss.

2.2.1 Bei der Variante „PBE Push" des PBE-Service wird eine E-Mail-Benachrichtigung an den Empfänger gesendet, in der die ursprüngliche E-Mail als verschlüsselter Anhang gespeichert ist. Nach der Online-Registrierung am Anfang kann der Empfänger die entschlüsselte E-Mail offline mittels einer Java-Anwendung auf seinem Desktop ansehen.

2.2.2 Bei der Variante „PBE Pull" des PBE-Service wird eine E-Mail-Benachrichtigung an den Empfänger gesendet. Der Empfänger kann die entschlüsselte E-Mail online über eine sichere SSL-Sitzung in seinem Browser ansehen, wenn er sich in einem sicheren Web-Portal einloggt und sein Passwort eingibt.

2.3 PBE ermöglicht Empfängern auch den Zugang zu einem sicheren Web-Portal sowie das Antworten auf eine verschlüsselte E-Mail in einem verschlüsselten Format.

2.4 Der Kunde kann das Portal, über das Empfänger ihre verschlüsselten E-Mails lesen, mit einem Branding versehen (zum Beispiel Kundenlogos und Support-Nummern hinzufügen).

2.5 Der Empfänger verschlüsselter E-Mails kann völlig neu entworfene E-Mail an PBE-Nutzer des Kunden senden.

2.6 Wenn der Kunde PBE E abonniert, steht ein Drittanbieter-Plugin für Outlook zur Verfügung, das der Outlook-Werkzeugleiste des Empfängers ein Symbol „Verschlüsseln" hinzufügt. Der Kunde anerkennt und stimmt zu, dass Symantec nicht für derartige Drittanbieter-Software verantwortlich ist.

2.7 Wenn der Kunde PBE E abonniert, kann ein Empfänger die Sprache des Secure-Web-Portals des Empfängers und der Benachrichtigungs-E-Mails aus einer Liste der unterstützten Sprachen auswählen.

3. Bereitstellung, Rechnungen und Änderungsanträge

3.1 Symantec beginnt mit der Rechnungsstellung für PBE ab dem Datum, an dem Symantec bestätigt, dass das Netzwerk des Kunden technisch in der Lage ist, PBE zu unterstützen ("technisches Genehmigungsdatum").

3.2 Klausel 5.2 in Anhang 1 kann nicht auf PBE angewendet werden. Symantec setzt sich zum Ziel, PBE-Bestellungen und -Änderungsanforderungen innerhalb von vier Wochen ab dem technischen Genehmigungsdatum auszuführen, vorausgesetzt, dass der Kunde alle Ermittlungen in Bezug auf das Vertragsobjekt mit der gebotenen Sorgfalt geführt hat.

3.3 Der Kunde erklärt sich bereit, sämtliche notwendigen Ressourcen, Informationen und Genehmigungen, wie jeweils erforderlich, verfügbar zu machen und seine DNS-Mail-Dienste hinsichtlich der Verbindung mit PBE zu aktivieren oder korrigieren.

3.4 Falls der Kunde „PBE Branding", „PBE Branding E" oder „PBE Branding Enterprise" abonniert, kann er das Branding des Portals maximal zweimal jährlich ändern.

4. Konfiguration

4.1 Der Kunde ist für die Implementierung der PBE-Konfiguration entsprechend den Wünschen des Kunden verantwortlich. Der Kunde konfiguriert PBE über ClientNet durch Wählen von unter dem Email-CC-Dienst verfügbaren Optionen.

4.2 Symantec betont, dass die PBE-Konfiguration vollständig der Kontrolle des Kunden unterliegt und dass die Genauigkeit dieser Konfiguration die Genauigkeit von PBE bestimmt. Symantec kann daher keine Haftung für sich direkt oder indirekt aus Fehlern von PBE hinsichtlich der Erfüllung der Verschlüsselungspflichten des Kunden ergebende Schäden oder Verluste übernehmen.

5. Dienstparameter

5.1 Folgende Einschränkungen sind auf PBE anwendbar:

5.1.1 Die Zahl der sicheren E-Mails, die Kunden monatlich über PBE Z versenden dürfen, darf nicht dreihundert (300) Mal die eingetragene Nutzung für PBE überschreiten. Die Zahl der sicheren E-Mails, die Kunden monatlich über PBE E versenden dürfen, darf nicht vierhundertachtzig (480) Mal die eingetragene Nutzung für PBE überschreiten. Beim Versenden an mehrere Empfänger wird jede eindeutige Adresse als eine sichere E-Mail gezählt. Falls der Kunde die Zahl der zulässigen sicheren E-Mails pro Monat überschreitet, erhöht Symantec die eingetragene Nutzung dementsprechend. Wenn Symantec die eingetragene Nutzung erhöht, stellt Symantec im eigenen Ermessen zusätzliche Rechnungen aus und/oder passt spätere Rechnungen entsprechend an, um die Gebühren für die Erhöhung der eingetragenen Nutzung anteilig für die Restdauer des momentanen Abrechnungszeitraums abzudecken.

5.1.2 Über PBE Z geleitete E-Mails sind komprimiert auf eine maximale Größe von fünfzig Megabyte (50 MB) pro E-Mail beschränkt. Über PBE E geleitete E-Mails sind auf eine maximale Größe von fünfzig Megabyte (50 MB) pro E-Mail-Nachverschlüsselung beschränkt.

5.1.3 Der Service Level für die E-Mail-Latenz in dem Service Level Agreement ist nicht auf PBE anwendbar.

5.1.4 Die Mindestanzahl der Nutzer von PBE Z beträgt 50 Nutzer. Anfangs- und Nachbestellungen von PBE Z können für Mindestblöcke von 50 Nutzern oder bei Bestellungen über 50 Nutzer in weiteren Stufen von 10 Nutzern erfolgen.

5.1.5 **PBE FUNKTIONIERT NUR BEI DER VERWENDUNG ZUSAMMEN MIT DEN DIENSTEN BE UND EMAIL CC UND FUNKTIONIERT NICHT ALS EIGENSTÄNDIGER DIENST. JEDER EINZELNE PBE-BENUTZER MUSS EIN EMAIL-CC-BENUTZER SEIN.**

6. Geschäftsbedingungen

6.1 DER KUNDE BESTÄTIGT UND AKZEPTIERT, DASS DIE PBE-NUTZUNG VOLLSTÄNDIG DER KONTROLLE UND IM ERMESSEN DES KUNDEN LIEGT. Die Nutzung von PBE ist allein dafür vorgesehen, dass der Kunde befähigt wird, eine vorhandene, effektiv implementierte akzeptable Computernutzungsrichtlinie (oder deren Entsprechung) umzusetzen. Die Nutzung verschlüsselter Dienste kann in einigen Ländern gesetzlichen Vorschriften unterworfen sein. Dem Kunden wird anempfohlen, vor der Nutzung von PBE stets die jeweils anwendbaren gesetzlichen Vorschriften zu prüfen. Symantec kann keinerlei Haftung für die zivilrechtliche oder strafrechtliche Verantwortlichkeit übernehmen, die dem Kunden gemäß den anwendbaren Gesetzen aufgrund der Nutzung des PBE Service entsteht.

K – Der Symantec Email Continuity.cloud Service („EC“)

1. EC im Überblick
1.1 EC ist ein Reserve-Nachrichtenaustauschsystem für die Umgebungen Microsoft Exchange und Lotus Notes. EC synchronisiert wichtige System- und Nutzerdaten, unter anderem das E-Mail-Verzeichnis und die persönlichen Kontakte einzelner Nutzer. Der Kunde kann EC darüber hinaus für die Unterstützung von BlackBerry®-Geräten mittels drahtloser Weiterleitung unter Verwendung des BlackBerry® Web Client oder BlackBerry® Internet Service sowie für die Integration in Outlook für Nutzer des Cached Mode in Outlook 2003 oder Outlook 2007 über eine installierte Outlook-Erweiterung einrichten.
1.2. *Unterstützte Versionen*: Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007, Lotus Notes Version 6, Lotus Notes Version 7.
1.3 *Unterstützte Versionen für Outlook-Erweiterung*: Microsoft Outlook 2003 im Cached Mode; Microsoft Outlook 2007 im Cached Mode.
1.4 Der Kunde verpflichtet sich, die erforderliche Hardware und Software (wie im Bereitstellungsformular angegeben) bereitzustellen und zu verwalten.

2. Beschreibung des EC-Dienst
2.1. *Aktivierung*. Der Kunde kann die Aktivierung von EC telefonisch beim Kundendienst von Symantec oder über das Portal E-Mail Management Services („EMS“) anfordern. Nach Aktivierung von EC erhält der Kunde per SMS Benachrichtigungen an von ihm genannte Mobiltelefone und persönliche E-Mail-Adressen. Zu diesem Zeitpunkt beginnt EC, eingehende E-Mails zu empfangen und zu sortieren, sie (vorbehaltlich Absatz 3.4; siehe unten) gegebenenfalls entsprechend anderen vom Kunden abonnierten E-Mail-Dienste von Symantec (z. B. E-Mail AV Dienst) zu filtern und an die entsprechenden Nutzerpostfächer weiterzuleiten. EC sorgt für bis zu dreißig (30) Tage nach der Deaktivierung für die Speicherung und Aufbewahrung von während der Aktivierung gesendetem und empfangenem E-Mail-Verkehr, sodass der Kunde diese E-Mails, sofern gewünscht, in sein primäres Mailsystem übernehmen kann.
2.2 *Aufbewahrung*. Der Kunde ist für die Festlegung der Nutzer, für die EC gelten soll, sowie des anzugebenden Aufbewahrungszeitraums für jeden dieser Nutzer verantwortlich. Die aufbewahrten E-Mails werden (a) nach Ablauf des festgelegten Aufbewahrungszeitraums für diese Nutzer, (b) nach Kündigung von EC gelöscht; maßgeblich ist dabei der zuerst eintretende Fall. Der Kunde muss ausreichend großen Speicherplatz erwerben, um den Aufbewahrungsanforderungen gemäß Klausel 4.1 unten gerecht zu werden.
2.3 *Authentication Manager.* Der Kunde kann seine Sicherheitsrichtlinie für die Authentifizierung durch Microsoft Active Directory auf EC erweitern, indem er es Nutzern ermöglicht, sich mit ihren Windows-Kennwörtern bei ihren EC-Postfächern anzumelden, sodass die Notwendigkeit eines gesonderten EC-Kennworts entfällt. Die Windows-Authentifizierung setzt die Verfügbarkeit eines zum Zeitpunkt der Aktivierung von EC für den Authentication Manager zugänglichen Windows-Domänencontrollers voraus, der zur Authentifizierung von Nutzern bei der Anmeldung an EC-Postfächern in der Lage ist. Unterstützte Versionen: Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007.
2.4 Das vom Kunden zu erwerbende Mindestkontingent an EC-Nutzern beläuft sich (a) auf eine Anzahl von Nutzern, die der Anzahl der Postfächer in der Microsoft Exchange-Umgebung des Kunden entspricht, oder (b) auf zehn (10) Nutzer, wobei die jeweils größere Anzahl ausschlaggebend ist.

3. Konfiguration
3.1 *Teilaktivierung*: Bei bestimmten E-Mail-Systemen/Versionen (Umgebungen Microsoft Exchange 2000, 2003 und 2007) kann EC für Teilbereiche der Umgebung des Kunden (eine oder mehrere Personen, ein oder mehrere Server und/oder ein oder mehrere Standorte) aktiviert werden; durch eine solche Teilaktivierung können örtlich begrenzte E-Mail-Ausfälle abgefangen werden.
3.2 *Aktivierung*: Ein Abonnement von EC berechtigt den Kunden zu vierundzwanzig (24) Aktivierungsvorgängen pro Jahr für einen Zeitraum von jeweils bis zu zwölf (12) aufeinanderfolgenden Stunden („inbegriffene Aktivierungen“). (So würde beispielsweise eine einzelne Aktivierung für einen Zeitraum von sechs (6) Stunden als ein (1) Aktivierungsvorgang und eine einzelne Aktivierung für einen Zeitraum von neunzehn (19) Stunden als zwei (2) Aktivierungsvorgänge zählen.) Wenn der Kunden die Höchstzahl inbegriffener Aktivierungen verbraucht hat, kann der Kunde zusätzliche Aktivierungen (für einen Zeitraum von jeweils zwölf (12) aufeinanderfolgenden Stunden) zu den zum betreffenden Zeitpunkt geltenden Tarifen von Symantec erwerben.
3.3 Systemtests: Die Systemtests umfassen (a) pro Vierteljahr einen (1) Test von EC für alle Nutzer mit einer Dauer von bis zu vier (4) Stunden sowie (b) für Umgebung mit Microsoft Exchange 2000, Microsoft Exchange 2003 oder Microsoft Exchange 2007 unbegrenzte Teiltests für bis zu zehn Prozent (10 %) der Nutzer. Der Kunde muss den Termin für diese Tests mindestens sieben (7) Geschäftstage vor dem vom Kunden gewünschten Testdatum mit Symantec abstimmen.
3.4 **DER KUNDE NIMMT ZUR KENNTNIS UND ERKLÄRT SICH DAMIT EINVERSTANDEN, DASS DIE VOM KUNDEN ABONNIERTEN SCANNING-DIENSTE VON SYMANTEC FÜR ANKOMMENDE UND ABGEHENDE E-MAILS UMGANGEN WERDEN, WENN SICH DER KUNDE IN EINEM AKTIVIERTEN ZUSTAND BEFINDET UND DER KUNDE DARAUFHIN E-MAILS AN EINE ANDERE, EBENFALLS IN EINEM AKTIVIERTEN ZUSTAND BEFINDLICHE ORGANISATION SENDET ODER VON DIESER EMPFÄNGT.**
3.5 Falls der Kunde die Services Email AV, Email AS, Email CC und/oder Email IC nutzt, kann Symantec innerhalb von ClientNet das Failover-Routing für die E-Mails des Kunden in die EC-Umgebung konfigurieren. Dieses Failover-Routing wird verwendet, wenn der EC Service aktiviert ist.
3.6 **FALLS DER KUNDE DIE SERVICES EMAIL AV, EMAIL AS, EMAIL CC ODER EMAIL IC NICHT NUTZT, IST DER KUNDE DAFÜR VERANTWORTLICH, DAS FAILOVER-ROUTING FÜR DIE E-MAILS DES KUNDEN IN DIE EC-UMGEBUNG ZU KONFIGURIEREN UND ZU PRÜFEN. DIESE FAILOVERS MÜSSEN IM RAHMEN DES BEREITSTELLUNGSPROZESSES ENTSPRECHEND DEN ANWEISUNGEN VON SYMANTEC EINGERICHTET UND DANACH BEIBEHALTEN WERDEN. FÜR DEN FALL, DASS DER KUNDE ES VERSÄUMT, DIESE FAILOVERS EINZURICHTEN ODER BEIZUBEHALTEN, ANERKENNT UND AKZEPTIERT DER KUNDE, DASS DAS ROUTING VON E-MAILS ZU EC NICHT MÖGLICH IST.**

4. Optionen
4.1 *Symantec Email Continuity.cloud Storage Option (Speicherplatz)*.
4.1.1 Der Kunde muss zu Aufbewahrungszwecken ausreichend großen Speicherplatz erwerben.
4.1.2 Falls der Kunde eines der Pakete Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud oder Symantec MessageLabs Ultimate Safeguard.cloud abonniert, enthält das Paket für die Dienste Symantec Email Continuity.cloud und Symantec Email Continuity Archive.cloud zusammen neuen E-Mail-Speicherplatz von maximal 0,7GB pro Benutzer pro Jahr. Falls der neue E-Mail-Speicherplatz des Kunden diese zulässige Speicherkapazität überschreitet, muss der Kunde für den Dienst zu den jeweils geltenden Preisen von Symantec ausreichend großen Speicherplatz erwerben.
4.1.3 Falls der Kunde nicht eines der in Klausel 4.1.2 aufgeführten Pakete abonniert, umfasst der Preis pro Benutzer keinen Speicherplatz, und der Kunde muss für den Dienst zu den jeweils geltenden Preisen von Symantec ausreichend großen Speicherplatz erwerben.

4.1.4 Wenn der Kunde zusätzlichen Speicherplatz erwerben muss, wird Symantec zusätzliche Rechnungen ausstellen und/oder spätere Rechnungen entsprechend anpassen, um die Kosten für die Speicherplatzerweiterung anteilig für die Restdauer des momentanen Abrechnungszeitraums abzudecken.

4.2 *Symantec Email Continuity.cloud Wireless Option*.

4.2.1 Wenn der Kunde die Option Symantec Email Continuity.cloud Wireless Option abonniert, können Systemadministratoren einzelne BlackBerry®-Geräte unter Verwaltung durch RIM BlackBerry® Enterprise Server (BES) bereitstellen. Wenn EC aktiviert ist, erfolgt das Senden und Empfangen von E-Mails durch BlackBerry®-Geräte weiterhin im Datenaustausch mit EMS, und zwar über einen vom BES-Server eingerichteten sicheren Kanal.

4.2.2. Unterstützte Versionen: Microsoft Exchange 2000, Microsoft Exchange 2003 oder Microsoft Exchange 2007; BlackBerry® Enterprise Server ab Version 4.0; Handheld-Geräte von BlackBerry® mit Firmware ab Version 4.1.

5. Allgemeine Bedingungen für EC

5.1 DER KUNDE IST SICH DER TATSACHE BEWUSST, DASS KEIN AUSFALLSICHERHEITSSERVICE FÜR E-MAILS EINEN HUNDERTPROZENTIGE SYNCHRONISIERUNG GARANTIEREN KANN. SYMANTEC KANN DAHER NUR DIE MASSNAHMEN ZUR LEISTUNGSERBRINGUNG ERGREIFEN, DIE GEGENWÄRTIGEN BRANCHENSTANDARDS ENTSPRECHEN.

5.2 Symantec weist ausdrücklich darauf hin, dass die Konfiguration von EC vollständig der Kontrolle des Kunden unterliegt. Die Nutzung von EC ist allein dafür vorgesehen, dass dem Kunden ermöglicht wird, eine vorhandene, effektiv implementierte akzeptable Computernutzungsrichtlinie (oder deren Entsprechung) umzusetzen. In manchen Ländern ist es unter Umständen notwendig, die Zustimmung einzelner Mitglieder des Personals dafür einzuholen. Symantec rät dem Kunden, vor dem Einsetzen von EC stets die regional geltenden Gesetze zu überprüfen. Symantec übernimmt keine Haftung für eine zivil- oder strafrechtliche Haftung des Kunden infolge der Nutzung von EC.

6. Softwarelizenz

6.1 Lizenzgewährung

Vorbehaltlich der Bedingungen dieses Vertrags gewährt Symantec dem Kunden das nicht ausschließliche, nicht übertragbare Recht zur Installation und Nutzung der Software für EC unter Beschränkung auf die eigenen internen Geschäftsvorgänge des Kunden („Software" bezeichnet jedes Softwareprogramm von Symantec für EC im Objektcode-Format, das von Symantec lizenziert wird und das den Bedingungen des Vertrags unterliegt, insbesondere neue Versionen oder Aktualisierungen, die im Rahmen dieses Vertrages bereitgestellt werden). Alle geistigen Eigentumsrechte an der Software sind und bleiben Eigentum von Symantec (und/oder von deren Zulieferern). Der Software wird von Symantec lizenziert und nicht verkauft. Der Kunde erkennt an, dass die Software und alle damit in Zusammenhang stehenden Informationen, insbesondere Aktualisierungen, Eigentum von Symantec und von deren Zulieferern sind. Der Kunde ist für die Einhaltung der Bedingungen dieses Vertrags oder für deren Verletzung durch jeden einzelnen Endnutzer verantwortlich und uneingeschränkt haftbar. Der Kunde setzt Symantec unverzüglich von einer unbefugten Nutzung oder von einer Verletzung der Bedingungen dieser Lizenz in Kenntnis.

6.2. Einschränkungen hinsichtlich des Kopierens und der Nutzung

Der Kunde kann die Software unter den folgenden Bedingungen herunterladen und installieren:

6.2.1. Der Kunde darf die Software nicht für mehr als die Anzahl von durch den Kunden lizenzierten Endnutzerlizenzen herunterladen oder installieren („Endnutzer" bezeichnet den physischen Computer, auf dem die Software installiert ist).

6.2.2. Der Kunde darf die Software, soweit dies billigerweise erforderlich ist, für Zwecke der Datensicherung, der Archivierung oder der Wiederherstellung im Notfall kopieren. Eine gedruckte Dokumentation darf vom Kunden nur für den internen Gebrauch vervielfältigt werden („Dokumentation" bezeichnet in der heruntergeladenen Software enthaltene Nutzerhandbücher und/oder Handbücher zur Bedienung der Software von Symantec.).

6.2.3 Dem Kunden wie auch mit dessen Billigung handelnden Dritten ist es untersagt: (i) die Software ohne vorherige schriftliche Genehmigung von Symantec zu dekompilieren, zu disassemblieren oder rückzuentwickeln, soweit dies nicht nach geltendem Recht ausdrücklich zulässig ist; (ii) Produktkennzeichnungen oder Hinweise auf Eigentumsrechte zu entfernen; (iii) die Software zu vermieten, zu verleihen oder zu Timesharing- oder Servicebüro-Zwecken zu nutzen; (iv) die Software zu verändern, zu übersetzen, anzupassen oder Bearbeitungen davon zu erstellen oder (v) die Software in anderer Weise zu nutzen oder zu kopieren, soweit dies hier nicht ausdrücklich vorgesehen ist.

6.3. Übertragung von Rechten

Der Kunde darf die Softwarelizenz aus diesem Vertrag ohne vorherige schriftliche Zustimmung von Symantec nicht übertragen, abtreten oder weitergeben. Jegliche Übertragung, Abtretung oder Weitergabe entgegen dieser Bestimmung ist nichtig.

6.4. Beschränkte Gewährleistung und Haftungsausschluss

6.4.1 Symantec gewährleistet, dass nach dem Herunterladen die Software in allen wesentlichen Gesichtspunkten der aktuellen Dokumentation von Symantec entspricht.

6.4.2 Die vorstehende Gewährleistung gilt nicht, wenn: (i) die Software nicht gemäß diesem Vertrag oder der Dokumentation genutzt wird; (ii) die Software oder Teile davon durch einen anderen Rechtsträger als durch Symantec verändert wurden oder (iii) eine Fehlfunktion in der Software durch Anlagen oder Geräte des Kunden oder durch fremde Software verursacht wurde.

6.4.3 DIE HAFTUNG VON SYMANTEC FÜR VERLETZUNGEN DER OBIGEN GEWÄHRLEISTUNG BESCHRÄNKT SICH EINZIG UND AUSSCHLIESSLICH AUF DEN ERSATZ DER SOFTWARE, SOWEIT EIN ERSATZ VERFÜGBAR IST. SYMANTEC GEWÄHRLEISTET NICHT, DASS DER BETRIEB DER SOFTWARE EIN UNUNTERBROCHENER ODER FEHLERFREIER IST. SYMANTEC SCHLIESST AUSDRÜCKLICH VERTRAGLICHE, KONKLUDENTE UND SONSTIGE GEWÄHRLEISTUNGEN JEDER ART AUS, INSBESONDERE GEWÄHRLEISTUNGEN EINER DURCHSCHNITTSQUALITÄT, EINER ZUFRIEDENSTELLENDEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

6.5. Kündigung

Mit Kündigung von EC oder des Vertrags enden mit sofortiger Wirkung alle hier gewährten Rechte des Kunden zur Nutzung der Software; der Kunde muss alle Kopien der Software und der Dokumentation umgehend an Symantec zurückgeben oder vernichten.

L – Schemus Tool

1.1 Das Schemus-Tool ist eine Software, die Daten zwischen dem Verzeichnisserver des Kunden und den Symantec-Diensten , welche vom Kunden abonniert werden, synchronisiert.
1.2 Die Lizenz für das Schemus-Tool wird dem Kunden von der Schemus Limited mittels einer gesonderten Endbenutzer-Lizenzvereinbarung („EULA des Dritten“) erteilt.
1.3 Der Kunde bestätigt und erkennt an, dass der Zugriff auf das Schemus-Tool und dessen Nutzung davon abhängig sind, dass der Kunde die Geschäftsbedingungen der EULA der Schemus Limited (wovon eine Kopie auf Anfrage bei Symantec erhältlich ist) akzeptiert und einhält.
1.4 Beim Schemus-Tool handelt es sich um eine kontrollierte Technologie, die anwendbaren Ausfuhr- und Einfuhrgesetzen und -verordnungen unterliegt, wie in den Ausfuhrkontrollbestimmungen des Abschnitts „Allgemein“ des Vertrags genauer dargelegt . **DER KUNDE BESTÄTIGT UND ERKENNT AN, DASS ER VERPFLICHTET IST, (I) VOR DEM HERUNTERLADEN DER SOFTWARE, (II) VOR DER VERGABE DES LIZENZSCHLÜSSELS UND (III) DANACH EINMAL JÄHRLICH, FALLS VON SYMANTEC VERLANGT, EINE COMPLIANCE-ERKLÄRUNG (WOVON EINE KOPIE AUF ANFRAGE BEI SYMANTEC ERHÄLTLICH IST) ZU UNTERZEICHNEN**.
1.5 Symantec gibt keine weiteren (ausdrücklichen, stillschweigenden, gesetzlichen oder sonstigen) Garantien in Bezug auf das Schemus-Tool ab. Falls ein Defekt in Bezug auf das Schemus-Tool auftritt, unternimmt Symantec wirtschaftlich angemessene Anstrengungen, um die Problemquelle zu ermitteln und das Problem gegebenenfalls an die Schemus Limited zu eskalieren.
1.6 Die Höchsthaftung von Symantec gegenüber dem Kunden in Bezug auf das Schemus-Tool ist auf eine Summe entsprechend dem vom Kunden an Symantec für das Schemus-Tool tatsächlich gezahlten Betrag oder einen Betrag von €350 begrenzt, wobei der höhere Betrag der jeweils maßgebliche Betrag ist.

M – Symantec MessageLabs Instant Messaging Security.cloud Service („IMSS“)

1 Überblick

1.1 Der Kunde muss sein Benutzerverzeichnis mit Symantec synchronisieren, um eine Liste mit Active-Directory-Benutzernamen und entsprechenden Instant-Message-(IM-)Benutzernamen innerhalb von ClientNet zu erstellen. Ein „interner Benutzer“ ist ein im Kundenverzeichnis bekannter und in die IMSS-Verwaltungsschnittstelle hochgeladener Benutzer. Ein „externer Benutzer“ ist ein im Kundenverzeichnis unbekannter und/oder nicht in die IMSS-Verwaltungsschnittstelle hochgeladener Benutzer.

1.2 Der Kunde muss ferner einfache Firewall-Änderungen vornehmen, um seine IM-Gespräche über Symantec zu steuern.

1.3 Sobald IMSS gemäß den Klauseln 1.1 und 1.2 oben konfiguriert wurde, werden Sofortnachrichten (Instant Messages) von internen Benutzern an externe Benutzer und umgekehrt über IMSS gesteuert, um von führenden Produkten gescannt zu werden, etwa von Skeptic™, der Symantec-eigenen heuristischen Scanvorrichtung.

1.4 IMSS kann nur bestimmte Versionen öffentlicher IM-Clients scannen. Symantec veröffentlicht die Liste mit unterstützten Versionen öffentlicher IM-Clients über ClientNet. Der Kunde bestätigt und erkennt an, dass Symantec diese Liste in regelmäßigen Zeitabständen ohne Vorankündigung aktualisieren und ändern kann.

1.5 Falls eine **eingehende** Sofortnachricht

1.5.1 annahmegemäß einen Virus oder sonstigen böswilligen Code enthält, wird sie blockiert;

1.5.2 eine URL-Adresse für eine Webseite enthält, auf der ein Virus oder anderer böswilliger Code entdeckt wurde, wird der Zugriff auf diese Webseite verweigert.

1.6 IMSS bietet auch eine einfache Anti-Phishing-Funktion, über die **eingehende** Sofortnachrichten, die für Phishing-Angriffe gehalten werden, blockiert werden können.

1.7 IMSS kann bestimmte Versionen von Word-, Excel- und PowerPoint-Dateien scannen, jedoch keine sonstigen Anhänge.

1.8 IMSS kann keine verschlüsselten Sofortnachrichten scannen.

2. IMSS-Inhaltskontrolle

2.1 IMSS ermöglicht, dass der Kunde seine eigene regelbasierte Inhaltefilterungsstrategie für ein- und ausgehende Sofortnachrichten konfigurieren kann.

2.2 Der Kunde ist für die Implementierung der Konfigurationsoptionen in Übereinstimmung mit der Richtlinie über akzeptable Computernutzung des Kunden (bzw. einer entsprechenden Vorgabe) über ClientNet verantwortlich. Die Regeln können auf der Grundlage von Gruppen oder Einzelpersonen konfiguriert werden. Vom Kunden an den Regeln vorgenommene Änderungen werden binnen vier (4) Stunden wirksam.

2.3 Es stehen Optionen zum Definieren der Aktion zur Verfügung, die beim Erkennen kontrollierter Inhalte in einer Sofortnachricht durchzuführen ist. Diese Optionen sind in ClientNet und in der aktuellen Version des Administratorhandbuchs ausführlich beschrieben.

2.4 Der Kunde kann die Ergebnisse seiner Regeln über ClientNet in Form täglicher, wöchentlicher, monatlicher und jährlicher Zusammenfassungen einsehen, die sowohl über die Regel als auch über den Benutzer organisiert werden.

3 Protokolle und Speicherung

3.1 Wenn der Kunde die Protokollfunktion aktiviert hat, erstellt Symantec tägliche Protokolle zu gescannten Sofortnachrichten. In jedem Protokoll sind Daten- und Zeitstempel, Inhalte sowie die Namen der übertragenen Dateien aufzuführen. Protokolle, die dem Kunden nicht zugestellt werden können, sind einunddreißig (31) Tage lang zu speichern und anschließend zu vernichten.

3.2 Der Kunde kann IMSS auch so konfigurieren, dass eine Kopie jeder Sofortnachricht an die kompatible Archiv- oder Speicherungslösung des Kunden gesendet wird.

4 Mitteilungen

4.1 Der Kunde kann IMSS so konfigurieren, dass automatisch Mitteilungen versendet werden:

4.1.1 an den Absender und den vorgesehenen Empfänger, falls eine Sofortnachricht blockiert wird, wenn angenommen wird, dass sie einen Virus enthält oder mit einem Phishing-Angriff oder kontrolliertem Inhalt einhergeht; oder

4.1.2 an den Empfänger, falls der Zugriff auf eine Website verweigert wird, da angenommen wird, dass sie einen Virus oder böswilligen Inhalt enthält.

4.2 Der Kunde kann Mitteilungen über ClientNet aktivieren, individuell anpassen und deaktivieren.

5 Support

5.1 Die Supportleistungen umfassen:

5.1.1 Begehung der IMSS-Schnittstelle, einschließlich Dienstbeschreibung und Frage-und-Antwort-Session. (Nicht dazu gehört die Unterstützung bei der Einrichtung von Regeln oder Analysen der Wirksamkeit von Regeln);

5.1.2 Administratorhandbuch;

5.1.3 Benutzerhandbuch.

6 IMSS-Geschäftsbedingungen

6.1 Vorgeschlagene Wortlisten und Vorlagenregeln für die Inhaltskontrolle, die Symantec zur Verfügung stellt, könnten Wörter enthalten, die als beleidigend betrachtet werden.

6.2 Der Kunde akzeptiert, dass Symantec berechtigt ist, unter Heranziehung von Wörtern, die individuellen Wortlisten des Kunden entnommen werden, Standardwortlisten zu erstellen und veröffentlichen.

6.3 Der Kunde erkennt an, dass E-Mails personenbezogene Informationen enthalten können und die Protokollierung und der Abfang von Sofortnachrichten deshalb einer Verarbeitung personenbezogener Daten gleichkommen können. Daher erkennt der Kunde an, dass IMSS ein konfigurierbarer Dienst ist und der Kunde für die IMSS-Konfiguration gemäß der Richtlinie über akzeptable Computernutzung des Kunden (bzw. einer entsprechenden Vorgabe) sowie allen anwendbaren Gesetzen oder Verordnungen allein verantwortlich ist. Folglich empfiehlt Symantec dem Kunden, vor der Nutzung von IMSS stets die vor Ort geltenden Gesetze zu prüfen und sicherzustellen, dass er und alle seine Mitarbeiter die Pflichten kennen und erfüllen, die sie hinsichtlich Datenschutzgesetzen und/oder -verordnungen deshalb haben, weil die Kunden IMSS nutzen. In bestimmten Ländern ist es unter Umständen notwendig, vor dem Abfangen und Protokollieren von Sofortnachrichten die Zustimmung einzelner Angestellter einzuholen. Der Kunde muss mindestens und mittels angemessener und minimaler individueller Anpassungen die Symantec-Standardmitteilungsfunktion für IMSS für diejenigen Personen implementieren, die ein zu IMSS gehörendes Kommunikationssystem nutzen. Sie (i) zeigt an, dass über dieses System übertragene Nachrichten protokolliert und unter Umständen abgefangen werden, (ii) weist auf die Zwecke der Protokollierung und des Abfangens hin und (iii) holt vor der Protokollierung und dem Abfangen die Zustimmung der Benutzer ein. Der Kunde darf Wörter, Sätze und Texte bezüglich der Elemente (i), (ii) und (iii) im vorhergehenden Satz im Rahmen kundenindividueller Anpassungen der Standardmitteilungsfunktion für IMSS übersetzen, jedoch nicht anderweitig ändern. Symantec übernimmt keine Haftung für eine zivil- oder strafrechtliche Haftung des Kunden, die sich daraus ergeben kann, dass der Kunde IMSS nutzt. Der Kunde stellt Symantec frei von sämtlichen Schadensersatzansprüchen seiner Mitarbeiter, von Dritten und/oder Regierungsbehörden im Zusammenhang damit, dass Symantec Sofortnachrichten abfängt bzw. protokolliert oder der Kunde Gesetze und/oder Verordnungen nicht einhält.

6.4 **DER KUNDE WIRD DARAUF AUFMERKSAM GEMACHT, DASS ÜBER IMSS GELEITETE SOFORTNACHRICHTEN GESCANNT UND IN HARDWARE-VORRICHTUNGEN GESPEICHERT WERDEN KÖNNEN, WELCHE SICH IN DEN VEREINIGTEN STAATEN VON AMERIKA BEFINDEN. DER KUNDE ERKLÄRT SICH FOLGLICH DAMIT EINVERSTANDEN, ALLE NOTWENDIGEN MASSNAHMEN ZU ERGREIFEN, UM (I) SEINE MITARBEITER, VERTRETER UND AUFTRAGNEHMER SOWIE DRITTE, DIE DAS ZU IMSS GEHÖRENDE KOMMUNIKATIONSSYSTEM NUTZEN, DARÜBER ZU INFORMIEREN, DASS JEGLICHE ÜBER IMSS ÜBERTRAGENE INFORMATIONEN, MÖGLICHERWEISE AUCH PERSONENBEZOGENE INFORMATIONEN ZU EINZELNEN PERSONEN, IN DEN VEREINIGTEN STAATEN VON AMERIKA VERARBEITET WERDEN KÖNNTEN; UND (II) DIE ZUSTIMMUNG DIESER MITARBEITER, VERTRETER, AUFTRAGNEHMER UND DRITTEN ZU EINER SOLCHEN VERARBEITUNG EINZUHOLEN, BEVOR ODER WÄHREND DER KUNDE IMSS AUSFÜHRT. FERNER KÖNNEN JEGLICHE PERSONENBEZOGENEN DATEN, DIE DER KUNDE SYMANTEC OFFENBART, AN MIT SYMANTEC VERBUNDENE UNTERNEHMEN UND/ODER UNTERAUFTRAGNEHMER VON SYMANTEC, DIE IM AUFTRAG VON SYMANTEC HANDELN, ÜBERTRAGEN WERDEN. DIESE VERBUNDENEN UNTERNEHMEN ODER UNTERAUFTRAGNEHMER KÖNNEN IHREN SITZ IN DEN VEREINIGTEN STAATEN ODER ANDEREN LÄNDERN HABEN, DIE UNTER UMSTÄNDEN WENIGER WEITREICHENDEN DATENSCHUTZGESETZEN UNTERWORFEN SIND ALS DER RECHTSKREIS, IN DEM DER KUNDE SEINEN SITZ HAT. IN DIESEM FALL WURDEN VON SYMANTEC MASSNAHMEN ERGRIFFEN, UM DIE ERFASSTEN DATEN BEI DEREN ÜBERTRAGUNG ANGEMESSEN ZU SCHÜTZEN. DER KUNDE VERPFLICHTET SICH, ALLE NOTWENDIGEN MASSNAHMEN ZU ERGREIFEN, UM (I) ALLE SEINE MITARBEITER, VERTRETER UND AUFTRAGNEHMER SOWIE DRITTE, ÜBER DIE DER KUNDE GEGENÜBER SYMANTEC PERSONENBEZOGENE DATEN OFFENBART, DARÜBER ZU INFORMIEREN, DASS DEREN DATEN IN DIESEN LÄNDERN VERARBEITET WERDEN KÖNNTEN; UND (II) DIE ZUSTIMMUNG DIESER MITARBEITER, VERTRETER, AUFTRAGNEHMER UND DRITTEN ZU EINER SOLCHEN VERARBEITUNG EINZUHOLEN. SYMANTEC LEHNT EINE HAFTUNG FÜR ENTSPRECHENDE VERSTÖSSE GEGEN ANWENDBARE GESETZE ODER VERORDNUNGEN AB.**

6.5 **KEINE SOFTWARE BZW. KEIN DIENST KANN EINE 100%-IGE ERKENNUNGSRATE GARANTIEREN. DESHALB ÜBERNIMMT SYMANTEC KEINE HAFTUNG FÜR SCHÄDEN ODER VERLUSTE, DIE DIREKT ODER INDIREKT DARAUF ZURÜCKZUFÜHREN SIND, DASS IMSS SPAM FÜR IM, VIREN, PHISHING-ANGRIFFE, BÖSWILLIGEN CODE, BLOCKIERTE URL-ADRESSEN ODER KONTROLLIERTE INHALTE NICHT ERKENNT ODER DASS IMSS SOFORTNACHRICHTEN FÄLSCHLICHERWEISE ALS SPAM FÜR IM, VIREN, PHISHING-ANGRIFFE, BÖSWILLIGEN CODE, BLOCKIERTE URL-ADRESSEN ODER KONTROLLIERTE INHALTE ENTHALTEND IDENTIFIZIERT.** Weiterhin wird die Konfiguration von IMSS-Inhaltskontrollregeln vollständig vom Kunden kontrolliert, und die Genauigkeit einer solchen Konfiguration wirkt sich auf die IMSS-Genauigkeit aus.

N – Symantec Email Continuity Archive.cloud and Symantec Email Continuity Archive Lite.cloud

1. Überblick
1.1 Der Symantec Email Continuity Archive.cloud und Symantec Email Continuity Archive Lite.cloud Service sind gehostete E-Mail-Speicherungssysteme, mit denen die Systemadministratoren des Kunden bestimmte E-Mail-Aufbewahrungsrichtlinien für die Speicherung archivierter E-Mails für eine Menge eigens dafür vorgesehener E-Mail-Postfächer festlegen können.

2. Kundenpflichten
2.1 Der Kunde ist für folgende Aktionen in Bezug auf den Dienst zuständig:
2.1.1 Bereitstellung und Wartung der notwendigen Hard- und Software (gemäß den Angaben im Bereitstellungsformular);
2.1.2 Sicherstellung, dass eine zweckgebundene technische Ressource mit Verwaltungsrechten zur Bereitstellung des Dienstes zur Verfügung steht;
2.1.3 Bestimmung, welche Benutzer zum Empfang des Dienstes berechtigt sein sollen, und der vorgegebenen Aufbewahrungszeit jedes dieser Benutzer;
2.1.4 Bestimmung und Schutz von Berechtigungen für den Zugriff auf das Archiv über die Kundenschnittstelle;
2.1.5 Festlegung und Verwaltung von Archivierungsaufbewahrungsrichtlinien;
2.1.6 Durchführung von Suchvorgängen für den Abruf archivierter Daten.
2.2 Falls der Kunde die zur Bereitstellung des Dienstes erforderlichen Aktionen binnen dreißig (30) Tagen ab dem Tag der Kundenbestellung nicht durchgeführt hat, kann Symantec anfangen, Kosten für den Dienst in Rechnung zu stellen.

3. Funktionen
3.1 Der *Symantec Email Continuity Archive.cloud Service* umfasst folgende Dienstfunktionen:
3.1.1 *E-Mail-Erfassung und -Speicherung* – E-Mails werden erfasst, sobald sie der primären E-Mail-Umgebung des Kunden zugestellt und in ein E-Mail-Archiv übertragen werden, um indexiert und gespeichert zu werden. E-Mails werden im Dienst verschlüsselt und gespeichert. E-Mail-Aufbewahrungsrichtlinien können für Benutzer festgelegt werden, um zu bestimmen, wann E-Mails in dem Dienst zu löschen sind.
3.1.2 *Wiederherstellung* – bietet die Möglichkeit zur Wiederherstellung von E-Mails aus dem E-Mail-Archiv zurück in die Exchange-Nachrichtenspeicher des Kunden.
3.1.3 *E-Discovery* – bietet den Systemadministratoren des Kunden die Möglichkeit, bestimmte Benutzer als „Prüfer" zu bestimmen und ihnen die Möglichkeit zu geben, zu Electronic-Discovery- und anderen Zwecken neben ihren eigenen auch E-Mails in anderen Postfächern zu überprüfen. Die Prüfer können ein Discovery-Archiv anlegen, das die Ergebnisse einer Suche in Benutzerpostfächern enthält. Das Discovery-Archiv kann in ein einzelnes Postfach exportiert werden.
3.1.4 *Windows-Authentifizierung* – ermöglicht Kunden, die Microsoft Exchange 2000, Microsoft Exchange 2003 und/oder Microsoft Exchange 2007 nutzen, die Sicherheitsrichtlinien des Kunden für die Microsoft-Active-Directory-Authentifizierung auf Benutzer des Dienstes auszuweiten, indem Benutzern die Möglichkeit gegeben wird, sich mittels ihres Active-Directory-Passworts am Dienst anzumelden.
3.1.5 *Endbenutzerarchiv* - ermöglicht von einer Aufbewahrungsrichtlinie erfassten Benutzern, von ihrem Postfach aus über eine webbasierte Schnittstelle auf ihr persönliches Archiv zuzugreifen, welches E-Mails enthält. Die E-Mail-Administratoren des Kunden können auch festlegen, ob Kunden E-Mails von ihrem persönlichen Archiv aus weiterleiten können oder nicht.
3.1.6 *Speicherungsverwaltung* – die Systemadministratoren des Kunden können eine Speicherungsverwaltungsrichtlinie definieren, mit der Anhänge aus den Exchange-Nachrichtenspeichern des Kunden zum Zweck der Reduzierung von Speicherungsanforderungen in den Dienst verschoben werden können.
3.2 Der *Symantec Email Continuity Archive Lite.cloud Service* umfasst folgende Dienstmerkmale (welche alle oben weiter beschrieben wird):
3.2.1 *E-Mail-Erfassung und -Speicherung*
3.2.2 *Wiederherstellung*
3.2.3 *E-Discovery*
3.2.4 *Windows-Authentifizierung*
Der Symantec Email Continuity Archive Lite.cloud Service umfasst nicht die Endbenutzerarchiv- oder Speicherungsverwaltungsfunktionen. Der Kunde kann auf die Endbenutzerarchiv-Dienstfunktion aufrüsten, indem er das *Symantec Email Continuity Archive Lite.cloud End User Pack (Endbenutzerpaket)* abonniert.
3.3 *Data Import Option* – Der Kunde ist berechtigt, Altdaten aus PST-Dateien in den Dienst zu importieren, indem er ein Import-Tool herunterlädt und anwendet. In diesem Zusammenhang ist die Entrichtung einer Importgebühr basierend auf der Menge der zu importierenden, erforderlichen Daten notwendig. Für den Fall, dass die tatsächlich vorhandene Menge Altdaten die Menge der erworbenen Importdaten übersteigt, behält Symantec sich das Recht vor, die Kosten für diese zusätzlichen Daten zu den jeweils geltenden Standardpreisen in Rechnung zu stellen.

4. Symantec Email Continuity.cloud Storage Option *(Speicherplatz)*
4.1 Der Kunde muss zu Aufbewahrungszwecken ausreichend großen Speicherplatz erwerben.
4.2 Falls der Kunde eines der Pakete Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud oder Symantec MessageLabs Ultimate Safeguard.cloud abonniert, enthält das Paket für die Dienste Symantec Email Continuity.cloud and Symantec Email Continuity Archive.cloud zusammen neuen E-Mail-Speicherplatz von maximal 0,7GB pro Benutzer pro Jahr. Falls der neue E-Mail-Speicherplatz des Kunden diese zulässige Speicherkapazität überschreitet, muss der Kunde für den Dienst zu den jeweils geltenden Preisen von Symantec ausreichend großen Speicherplatz erwerben.
4.3 Falls der Kunde nicht eines der in Klausel 4.2 aufgeführten Pakete abonniert, umfasst der Preis pro Benutzer keinen Speicherplatz, und der Kunde muss für den Dienst zu den jeweils geltenden Preisen von Symantec ausreichend großen Speicherplatz erwerben.
4.4 Wenn der Kunde zusätzlichen Speicherplatz erwerben muss, wird Symantec zusätzliche Rechnungen ausstellen und/oder spätere Rechnungen entsprechend anpassen, um die Kosten für die Speicherplatzerweiterung anteilig für die Restdauer des momentanen Abrechnungszeitraums abzudecken.

5. Geschäftsbedingungen
5.1 Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrentsprechender Anfertigung von Sicherungskopien eingetreten wäre.
5.2 Symantec übernimmt keine Haftung, falls der Dienst eventuell nicht gemäß der Beschreibung hierin bereitgestellt wird, was dadurch verursacht werden kann, dass (a) Symantec nicht seine Standardpraktiken beim Einsatz und der Verwaltung des Dienstes gegenüber

dem Kunden anwenden kann, (b) der Kunde die im Benutzerhandbuch oder Bereitstellungsformular dargelegten Symantec-Richtlinien nicht befolgt oder (c) der Kunde es versäumt, den Dienst zu aktivieren oder nutzen.

5.3 Symantec betont, dass die Konfiguration und die Nutzung des Dienstes vollständig der Kontrolle des Kunden unterliegen. Symantec empfiehlt, dass der Kunde über eine Richtlinie über akzeptable Computernutzung (bzw. eine entsprechende Vorgabe) verfügt. In bestimmten Ländern ist es unter Umständen notwendig, die Genehmigung von einzelnen Angestellten einzuholen. Symantec rät dem Kunden, vor der Nutzung des Dienstes stets die vor Ort geltenden Gesetze zu prüfen. Symantec übernimmt keine Haftung für eine zivil- oder strafrechtliche Haftung des Kunden infolge der Nutzung des Dienstes.

5.4 DER KUNDE AKZEPTIERT UND ERKENNT AN, DASS DER DIENST TEILWEISE ODER INSGESAMT IN DEN VEREINIGTEN STAATEN VON AMERIKA AUSGEFÜHRT WERDEN KÖNNTE UND DER KUNDE DAFÜR VERANTWORTLICH IST, ALLE FÜR DIE DATENÜBERTRAGUNG ERFORDERLICHEN BEWILLIGUNGEN UND GENEHMIGUNGEN EINZUHOLEN. DER KUNDE AKZEPTIERT FERNER UND ERKENNT AN, DASS SYMANTEC KEINE HAFTUNG FÜR ENTSPRECHENDE VERSTÖSSE GEGEN ANWENDBARE GESETZE BZW. VERORDNUNGEN ÜBERNIMMT.

5.5 Der Kunde bestätigt und stimmt darin überein, dass (i) die Symantec-Scandienste (Email AV, Email AS, Email IC und Email CC) nicht alle E-Mails scannen, die ursprünglich im Archiv eingehen, und (ii) die Symantec-Scandienste (Email AV, Email AS, Email IC und Email CC) keine E-Mails scannen, die aus dem Archiv für eine Wiederherstellung in Benutzerpostfächern freigegeben werden. Folglich lehnt Symantec jegliche Haftung für Viren, Spam, Bilder oder unangemessene Inhalte ab, die derartige wiederhergestellte E-Mails enthalten könnten. Das Service Level Agreement ist ferner nicht auf derartige wiederhergestellte E-Mails anwendbar.

5.6 Der Kunde bestätigt und stimmt zu, dass Symantec unter keinen Umständen die Funktion eines Drittanbieter-Downloaders im Sinne der SEC-Bestimmungen übernehmen kann.

6. Softwarelizenz

6.1 Lizenzgewährung

Vorbehaltlich der Bedingungen dieses Vertrags gewährt Symantec dem Kunden das nicht ausschließliche, nicht übertragbare Recht zur Installation und Nutzung der Software für den Symantec Email Continuity Archive.cloud Service oder den Symantec Email Continuity Archive Lite.cloud Service unter Beschränkung auf die eigenen internen Geschäftsvorgänge des Kunden („Software" bezeichnet jedes Softwareprogramm von Symantec für den Symantec Email Continuity Archive.cloud Service oder den Symantec Email Continuity Archive Lite.cloud Service im Objektcode-Format, das von Symantec lizenziert wird und das den Bedingungen des Vertrags unterliegt, insbesondere neue Versionen oder Aktualisierungen, die im Rahmen dieses Vertrages bereitgestellt werden). Alle geistigen Eigentumsrechte an der Software sind und bleiben Eigentum von Symantec (und/oder von deren Zulieferern). Der Software wird von Symantec lizenziert und nicht verkauft. Der Kunde erkennt an, dass die Software und alle damit in Zusammenhang stehenden Informationen, insbesondere Aktualisierungen, Eigentum von Symantec und von deren Zulieferern sind. Der Kunde ist für die Einhaltung der Bedingungen dieses Vertrags oder für deren Verletzung durch jeden einzelnen Endnutzer verantwortlich und uneingeschränkt haftbar. Der Kunde setzt Symantec unverzüglich von einer unbefugten Nutzung oder von einer Verletzung der Bedingungen dieser Lizenz in Kenntnis.

6.2. Einschränkungen hinsichtlich des Kopierens und der Nutzung

Der Kunde kann die Software unter den folgenden Bedingungen herunterladen und installieren:

6.2.1. Der Kunde darf die Software nicht für mehr als die Anzahl von durch den Kunden lizenzierten Endnutzerlizenzen herunterladen oder installieren („Endnutzer" bezeichnet den physischen Computer, auf dem die Software installiert ist).

6.2.2. Der Kunde darf die Software, soweit dies billigerweise erforderlich ist, für Zwecke der Datensicherung, der Archivierung oder der Wiederherstellung im Notfall kopieren. Eine gedruckte Dokumentation darf vom Kunden nur für den internen Gebrauch vervielfältigt werden („Dokumentation" bezeichnet in der heruntergeladenen Software enthaltene Nutzerhandbücher und/oder Handbücher zur Bedienung der Software von Symantec.).

6.2.3 Dem Kunden wie auch mit dessen Billigung handelnden Dritten ist es untersagt: (i) die Software ohne vorherige schriftliche Genehmigung von Symantec zu dekompilieren, zu disassemblieren oder rückzuentwickeln, soweit dies nicht nach geltendem Recht ausdrücklich zulässig ist; (ii) Produktkennzeichnungen oder Hinweise auf Eigentumsrechte zu entfernen; (iii) die Software zu vermieten, zu verleihen oder zu Timesharing- oder Servicebüro-Zwecken zu nutzen; (iv) die Software zu verändern, zu übersetzen, anzupassen oder Bearbeitungen davon zu erstellen oder (v) die Software in anderer Weise zu nutzen oder zu kopieren, soweit dies hier nicht ausdrücklich vorgesehen ist.

6.3. Übertragung von Rechten

Der Kunde darf die Softwarelizenz aus diesem Vertrag ohne vorherige schriftliche Zustimmung von Symantec nicht übertragen, abtreten oder weitergeben. Jegliche Übertragung, Abtretung oder Weitergabe entgegen dieser Bestimmung ist nichtig.

6.4. Beschränkte Gewährleistung und Haftungsausschluss

6.4.1 Symantec gewährleistet, dass nach dem Herunterladen die Software in allen wesentlichen Gesichtspunkten der aktuellen Dokumentation von Symantec entspricht.

6.4.2 Die vorstehende Gewährleistung gilt nicht, wenn: (i) die Software nicht gemäß diesem Vertrag oder der Dokumentation genutzt wird; (ii) die Software oder Teile davon durch einen anderen Rechtsträger als durch Symantec verändert wurden oder (iii) eine Fehlfunktion in der Software durch Anlagen oder Geräte des Kunden oder durch fremde Software verursacht wurde.

6.4.3 DIE HAFTUNG VON SYMANTEC FÜR VERLETZUNGEN DER OBIGEN GEWÄHRLEISTUNG BESCHRÄNKT SICH EINZIG UND AUSSCHLIESSLICH AUF DEN ERSATZ DER SOFTWARE, SOWEIT EIN ERSATZ VERFÜGBAR IST. SYMANTEC GEWÄHRLEISTET NICHT, DASS DER BETRIEB DER SOFTWARE EIN UNUNTERBROCHENER ODER FEHLERFREIER IST. SYMANTEC SCHLIESST AUSDRÜCKLICH VERTRAGLICHE, KONKLUDENTE UND SONSTIGE GEWÄHRLEISTUNGEN JEDER ART AUS, INSBESONDERE GEWÄHRLEISTUNGEN EINER DURCHSCHNITTSQUALITÄT, EINER ZUFRIEDENSTELLENDEN QUALITÄT ODER DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK.

6.5. Kündigung

Mit Kündigung des Symantec Email Continuity Archive.cloud Diensts oder des Symantec Email Continuity Archive Lite.cloud Diensts oder des Vertrags enden mit sofortiger Wirkung alle hier gewährten Rechte des Kunden zur Nutzung der Software; der Kunde muss alle Kopien der Software und der Dokumentation umgehend an Symantec zurückgeben oder vernichten.

7. Ablauf des Service und Datenextrahierung

7.1 Bei Ablauf/Kündigung des Symantec Email Continuity Archive.cloud Diensts oder des Symantec Email Continuity Archive Lite.cloud Diensts löscht Symantec die Daten des Kunden aus dem Archiv.

7.2 Der Kunde kann jederzeit vor Ablauf des Service seine Daten aus dem Archiv extrahieren.

O – Der Symantec MessageLabs Volume Mail Service (der „Massenmail-Dienst“)

1. Wenn der Kunde den Massenmail-Dienst abonniert, darf der Kunde Massenmails vorbehaltlich folgender Bedingungen versenden und empfangen:

1.1 Die Massenmail darf nur an bestätigte, erwünschte Opt-in-Empfänger gerichtet sein. Der Kunde muss auf Verlangen von Symantec sowie vorbehaltlich der geltenden Gesetze diese Bestätigungen nachweisen können.

1.2 Massenmails einschließlich der Anhänge dürfen eine Größe von 500 KB nicht überschreiten.

1.3 Das Feld ‚Empfänger' in jeder Massenmail darf nicht mehr als fünfhundert (500) E-Mail-Adressen enthalten.

1.4 Der Kunde muss ein effektives Listenverwaltungssystem führen, mit dem unter anderem E-Mail-Adressen unverzüglich entfernt werden können, die ungültig bzw. infolge einer Kündigung zu löschen sind.

1.5 Der Kunde muss den Symantec MessageLabs Email Anti-Virus.cloud Service für seine Standard-E-Mails empfangen.

1.6 Die Massenmails des Kunden müssen von einer von den Standard-E-Mails separaten Domäne ausgehen bzw. an eine solche Domäne gerichtet sein, wodurch möglich wird, dass die Massenmails an einen speziell bereitgestellten Control Tower gerichtet werden.

1.7 Der Standard-Banner für ausgehende Nachrichten benachrichtigt den Empfänger darüber, dass die Massenmail auf Viren überprüft wurde, enthält jedoch nicht das Symantec-Logo.

1.8 Falls der Kunde die Bereiche F oder G des Massenmail-Dienstes gemäß Abschnitt B „Dienst und Gebühren“ abonniert, ist er verpflichtet, die Menge der zu versendenden bzw. empfangenden Massenmails auf maximal 250.000 Empfänger pro Tag zu begrenzen.

1.9 Der Kunde erkennt an und akzeptiert, dass das Versenden von Massenmails mit Wahrscheinlichkeit wechselnde Auswirkungen auf die Fließeigenschaften des E-Mail-Verkehrs haben wird. Derartige Auswirkungen können von Symantec nicht kontrolliert werden; aus diesem Grund gelten die im Service Level Agreement aufgeführten Service Levels nicht für Massenmails.

1.10 Falls zu irgendeinem Zeitpunkt (i) die E-Mail-Systeme des Kunden auf eine Sperrliste gesetzt werden, (ii) der Kunde verursacht, dass die Symantec-Systeme auf eine Sperrliste gesetzt werden, weil Spam versendet wurde, oder (iii) der Kunde in dieser Anlage dargelegten Verpflichtungen nicht nachkommt, ist Symantec verpflichtet, den Kunden darüber zu informieren; in diesem Fall behält Symantec sich das Recht vor, im eigenen Ermessen umgehend die Bereitstellung der Dienste ganz oder teilweise zu verweigern bzw. vorübergehend auszusetzen oder ganz einzustellen.

1.11 Für jeden Massenmail-Dienstbereich gilt eine maximale Quote zulässiger Empfänger pro Monat. Diese Quoten sind nicht übertragbar oder addierbar; aus diesem Grund ist keine Übertragung ungenutzter Empfängerquoten auf nachfolgende Monate möglich.

1.12 Der Kunde hat Symantec zu benachrichtigen, wenn bei der tatsächlichen Massenmail- Nutzung zu irgendeiner Zeit die Zahl der pro Monat zulässigen Empfänger für den derzeit vom Kunden genutzten Bereich überschritten wird. Dies hat zur Folge, dass Symantec die Gebühr für den jeweiligen Bereich gemäß der jeweils aktuellen Preisliste von Symantec erhöhen wird. Darüber hinaus wird Symantec die tatsächliche Massenmail-Nutzung durch den Kunden überwachen; wenn die monatliche Zahl der Empfänger die für den derzeit vom Kunden genutzten Bereich zulässige Zahl überschreitet, wird Symantec die Gebühr gemäß der jeweils aktuellen Preisliste von Symantec erhöhen. Symantec wird im eigenen Ermessen zusätzliche Rechnungen ausstellen und/oder spätere vierteljährlich ausgestellte Rechnungen entsprechend anpassen, um die Gebühren für derartige Erhöhungen abzudecken.

P – Symantec Enterprise Vault.cloud

1. Übersicht

1.1 Symantec EV.cloud ist die Sammelbezeichnung für eine Reihe von Archivierungsdiensten (wie in den nachfolgenden Klauseln 1.1 bis 1.10 einschließlich beschrieben). Alle im Rahmen von Symantec EV.cloud bereitgestellten Services sind mit genehmigten Versionen von Exchange-Servern und gehosteten Exchange-Diensten kompatibel, die am Standort des Kunden installiert sind.
1.2 Folgendes gilt sowohl für den Symantec Enterprise Vault Personal.cloud Service als auch für den Symantec Enterprise Vault Discovery.cloud Service:
1.2.1 Die maximale Größe von E-Mails, die von Symantec Enterprise Vault Personal.cloud Service und Symantec Enterprise Vault Discovery.cloud Service aufgenommen werden können, beträgt 50 MB.
1.2.2 Folgendes gilt sowohl für den Symantec Enterprise Vault Personal.cloud Service als auch für den Symantec Enterprise Vault Discovery.cloud Service:
1.2.3 Kunden können Nachrichten im Archiv, die von einem der beiden Services erstellt wurden, direkt beantworten oder weiterleiten. Kunden können so regelmäßig Backup-Dateien für den Fall erstellen, dass ihr E-Mail-System ausfällt.
1.2.4 Keiner der Services ist ein Ersatz dafür, dass der Kunde ein lokales Backup seines Mail-Servers erstellen sollte. Falls der Kunde seinen Mail-Server wiederherstellen muss, sollte die Wiederherstellung mithilfe lokal verwalteter Daten und nicht mithilfe der im Archiv gespeicherten Daten erfolgen.

1.1. Symantec Enterprise Vault Personal.cloud

Der internetbasierte E-Mail-Archivierungsservice Symantec Enterprise Vault Personal.cloud wurde entwickelt, um Benutzern im Unternehmen des Kunden über Microsoft Outlook oder Outlook Web Access (sofern unterstützt) Zugriff auf ihre eigenen persönlichen E-Mail-Archive zu erteilen und ihnen so die Möglichkeit zu geben, verlorene oder gelöschte E-Mails zu suchen und wiederherzustellen.
1.1.1 Die ein- und ausgehende E-Mail-Kommunikation des Kunden, einschließlich Anlagen, wird in einem durchsuchbaren Online-Datenspeicher ("persönliches Archiv") gespeichert, das von Benutzern auf verloren gegangene oder gelöschte E-Mails durchsucht werden kann.
1.1.2 Benutzer können zudem über Microsoft Outlook, Outlook Web Access (sofern unterstützt), IBM Lotus Notes, BlackBerry®-Geräte und über eine browserbasierte sichere Website auf das persönliche Archiv zugreifen.
1.1.3 Es gibt zwei Möglichkeiten, das persönliche Archiv auf E-Mails und Anhänge zu durchsuchen: Benutzer können entweder die "Schnellsuche" (Quick Search) oder die "Erweiterte Suche" (Advanced Search) wählen. Mit der Option "Erweiterte Suche" können Benutzer ihre Suchvorgänge anhand verschiedenster Kriterien anpassen, wie etwa Schlüsselwörter im Nachrichtentext oder mit "An", "Von", "Betreff", "Datum" und Format des Anhangs.
1.1.4 Sofern die entsprechende Funktion aktiviert ist, können Benutzer (wie in Outlook oder Notes) Nachrichten direkt von Symantec Enterprise Vault Personal.cloud aus beantworten und weiterleiten.
1.1.5 Benutzer können Suchvorgänge anhand verschiedenster Kriterien (Datumsbereich, E-Mail-Absender, Art des Anhangs usw.) definieren und anschließend speichern, so dass sie die Suche nach Bedarf erneut ausführen können.
1.1.6 Die Legacy-E-Mail des Kunden wird in das persönliche Archiv verschoben, und die lokalen Archive werden entfernt. Auf diese Weise kann Speicherplatz auf den freigegebenen Laufwerken und E-Mail-Servern des Kunden zurückgewonnen werden.
1.1.7 Mithilfe des persönlichen Archivs des Kunden können ältere E-Mails bei Verlust oder Diebstahl eines Computers oder Laptops wiederhergestellt werden.
1.1.8 Kunden können PST-Dateien in Symantec Enterprise Vault Personal.cloud aufnehmen; dort wird die Ordnerstruktur nach der Erstaufnahme optional verwaltet.

1.2. Symantec Enterprise Vault Discovery.cloud

Der internetbasierte E-Mail-Archivierungsservice Symantec Enterprise Vault Discovery.cloud Service beschleunigt Anfragen zur rechtlichen Offenlegung (E-Discovery) und hilft Kunden, Richtlinien für die E-Mail-Aufbewahrung durchzusetzen sowie das Risiko bei Datenverlust zu mindern. Discovery Archive unterstützt Kunden bei der Aufbewahrung von E-Mails im Zusammenhang mit Rechtsstreitigkeiten und gesetzlichen Aufbewahrungsfristen und hilft, das besonders geschützte Vertrauensverhältnis zwischen Anwalt und Mandant zu wahren.
1.2.1 Symantec Enterprise Vault Discovery.cloud speichert und indiziert E-Mails, Anhänge und BlackBerry®-Nachrichten (SMS-Text, PIN-zu-PIN, Anrufprotokoll) in einem zentralen Online-Datenspeicher.
1.2.2 Kunden können zum Schutz ihrer Mitarbeiter gesetzliche Aufbewahrungsfristen für bestimmte Mitteilungen (auf der Basis von Suchkriterien) definieren oder mithilfe von automatisierten Löschrichtlinien verhindern, dass juristisch relevante E-Mails versehentlich gelöscht werden. Administratoren und Prüfer können der Verschwiegenheitspflicht unterliegende Anwalt-Mandanten-Mitteilungen kennzeichnen und so von etwaigen E-Discovery-Anfragen ausschließen.
1.2.3 Im Suchprotokoll des Symantec Enterprise Vault Discovery.cloud-Service werden alle Aktivitäten von Prüfern aufgezeichnet, damit Administratoren die relevanten Prüfungen durchführen können.
1.2.4 Administratoren können Benutzer nach spezifischen Kriterien zu Gruppen zusammenzufassen. Diese Gruppen können dann von Prüfern durchsucht werden.
1.2.5 Kunden können den Inhalt archivierter E-Mails und Anhänge anhand verschiedenster Suchkriterien durchsuchen, einschließlich der Nachrichtenfelder "An", "Von", "Datum", "Betreff" sowie Text, Anhängen und anderen Eigenschaften von Nachrichten.
1.2.6 Prüfer im Unternehmen des Kunden können durch Suchergebnisse navigieren, markierte Suchbegriffe identifizieren und potenziell gefährdende E-Mails kennzeichnen, so dass sie zur weiteren Prüfung leicht abrufbar sind.
1.2.7 Kunden können E-Mails im Zusammenhang mit einem bestimmten Rechtsstreit oder einer juristischen Angelegenheit kennzeichnen und zur weiteren Prüfung und Analyse in das Fallverwaltungssystem oder in andere Anwendungen eines Drittanbieters exportieren.
1.2.8 Prüfer im Unternehmen des Kunden können benutzerdefinierte E-Mail-Suchvorgänge auf der Basis der E-Mail-Richtlinien des Kunden definieren, speichern und nach Bedarf erneut ausführen.
1.2.9 Prüfer des Kunden können Richtlinienwarnungen definieren, um sich benachrichtigen zu lassen, wenn eine E-Mail Kriterien eines "gespeicherten Suchvorgangs" erfüllt (beispielsweise wenn bestimmte Wörter oder Ausdrücke in der Nachricht vorkommen).

1.3. Symantec Enterprise Vault.cloud Blackberry® Option

Mit dem internetbasierten Service Symantec Enterprise Vault.cloud Blackberry® Option können Benutzer über ihre BlackBerry®-Geräte auf archivierte E-Mails, Anhänge, SMS- und PIN-zu-PIN-Nachrichten sowie Anrufprotokolle zugreifen und sie durchsuchen. Der Service unterstützt Benutzer beim Suchen und Wiederherstellen verlorener oder gelöschter E-Mails und sorgt dafür, dass Benutzer ihr BlackBerry®-Gerät auch dann weiter zum Schreiben, Beantworten und Senden von Nachrichten in Echtzeit nutzen können, wenn der primäre E-Mail-Server des Kunden ausfällt. Symantec Enterprise Vault.cloud Blackberry® Option kann als zusätzliche Option zum Symantec Enterprise Vault Personal.cloud Service hinzugekauft werden.

1.3.1 Symantec Enterprise Vault.cloud Blackberry® Option kann von Administratoren über einen BlackBerry® Enterprise Server (BES) oder von Benutzern mithilfe des BlackBerry® Desktop Manager installiert werden.
1.3.2 Benutzer können sich durch Klicken auf das auf dem Startbildschirm ihres Blackberrys angezeigte Symbol bei Personal Archive for BlackBerry® einloggen.
1.3.3 Nach dem Klicken auf die Anwendung wird für drei Sekunden ein Begrüßungsbildschirm eingeblendet und der Benutzer anschließend zur Eingabe seiner Anmeldedaten aufgefordert.
1.3.4 Nach dem erfolgreichen Login wird der Benutzer zum Startbildschirm (d. h. zur Listenanzeige) des persönlichen Archivs weitergeleitet.
1.3.5 In der Listenanzeige (Mailbox) können Benutzer u. a. folgende Aufgaben ausführen: Verfassen neuer Nachrichten, Beantworten oder Weiterleiten von E-Mails und Durchführen einfacher oder erweiterter Suchvorgänge.
1.3.6 Benutzer können mithilfe einfacher oder erweiterter Suchvorgänge in allen Nachrichten und Anrufprotokollen ihres persönlichen Archivs nach alten, verloren gegangenen oder gelöschten E-Mails suchen und diese Nachrichten in ihrem Posteingang wiederherstellen.
1.3.7 Benutzer können Text in das Suchfeld eingeben und durch Aktivierung des Suchsymbols die Suche starten. Suchergebnisse können nach den Feldern "Datum", "Von" und "An" gefiltert werden.
1.3.8 Mithilfe ihres persönlichen Archivs können Benutzer auch dann Nachrichten schreiben, beantworten und senden, wenn die primäre E-Mail-Plattform (z. B. Microsoft Exchange) ausfällt.

1.4 AdvisorMail on Symantec.cloud™
Der internetbasierte E-Mail-Archivierungsservice AdvisorMail on Symantec.cloud™ (Advisor Mail) soll den durch bestimmte gesetzliche Vorschriften zur Auflage gemachten Prüfprozess beschleunigen. Der Advisor Mail Service archiviert E-Mails in einem zentralen Repository. Nachrichten werden in Übereinstimmung mit den Richtlinien des Kunden automatisch gescannt und gekennzeichnet. Nachrichten oder Anhänge, die bestimmte Schlüsselwörter oder Ausdrücke enthalten, können dann zur Richtliniendurchsetzung von Compliance-Verantwortlichen geprüft werden.
1.4.1 Advisor Mail zeichnet die gesendeten und empfangenen Nachrichten automatisch auf und leitet sie – mit TLS- oder VPM-Technologie sicher verschlüsselt – zur Aufbewahrung an mehrere Rechenzentren weiter. Dieser Vorgang erfordert kein Eingreifen seitens des Kunden.
1.4.2 Advisor Mail umfasst mehrere Verwaltungs- und Berichtsfunktionen, wie etwa Vor- oder Nachprüfungsmodi, Stichproben, anpassbare Regeln für bestimmte Domänen- oder E-Mail-Adressen und Übersichtsberichte.
1.4.3 Advisor Mail bietet zur Prüfung von E-Mail-Nachrichten zwei separate Berechtigungsstufen: Administrator (vollständiger Zugriff) und Auditor (Kontrollrechte für ausgewählte Mailboxen).
1.4.4 Das Funktionsangebot von Advisor Mail umfasst mehrere Tools zur Optimierung des Kontrollprozesses, darunter automatische Kennzeichnung verdächtiger E-Mails für die Kontrolle durch einen Prüfer (Auditor).
1.4.5 Kunden können ihren Startordner (z. B. Nachprüfung), Datumsbereich und Nachrichtenanzeige (z. B. Listen- oder Snippet-Anzeige) auswählen.
1.4.6 Mit der Funktion "Next Click" (Nächster Klick) können Benutzer mit nur einem Mausklick die nächste Richtlinienverletzung in den betreffenden E-Mail-Nachrichten und Anhängen ansteuern, während mit den Rechtsklick-Aktionen das Auswählen von Befehlen (z. B. Aufnahme von Schlüsselwörtern in das Wörterbuch) durch einfaches Klicken mit der rechten Maustaste ermöglicht wird.
1.4.7 Mit der mehrstufigen Kontrollfunktion in Advisor Mail können Kunden mit nur einem Befehl ein betriebseigenes Wörterbuch (Liste mit Wörtern und Ausdrücken, die einer Richtlinienverletzung entsprechen) an standortferne Büros weiterleiten.
1.4.8 Mit dem Editor für die Positivliste (Whitelist) in Advisor Mail können Kunden Schlüsselwörter und Ausdrücke, die häufig in Ausschlüssen (z. B. rechtliche Haftungsausschlüsse im Fußtext von E-Mail-Nachrichten) enthalten sind, in die Positivliste aufnehmen, um die Anzahl der Fehlerkennungen (False Positives) in Bezug auf Compliance-Verstößße zu reduzieren.
1.4.9 Mit Advisor Mail können Kunden E-Mail-Adressen hinzufügen, Benutzer anderen Büros zuweisen, Regeln ändern und mehrere E-Mails prüfen.
1.4.10 Das Suchprotokoll von Advisor Mail zeichnet die Überwachungsaktivitäten von Prüfern auf und unterstützt Administratoren so bei der Einhaltung von Compliance-Anforderungen.
1.4.11Prüfer können den Nachrichten nach Bedarf Notizen beifügen.

1.5 AdvisorMail IM Option on Symantec.cloud™
AdvisorMail IM Option on Symantec.cloud™ ist der internetbasierte Archivierungsservice von Symantec für unterstützte Instant Messaging-Plattformen. Instant Messages werden in Advisor Mail aufgezeichnet, gespeichert und indiziert und dann in Übereinstimmung mit den Compliance-Richtlinien des Kunden überwacht. Instant Messages, die bestimmte Schlüsselwörter oder Ausdrücke enthalten, können dann zur Richtliniendurchsetzung von Compliance-Verantwortlichen geprüft werden. AdvisorMail IM Option on Symantec.cloud™ kann als zusätzlicher Service optional zu Advisor Mail hinzugekauft werden
1.5.1 AdvisorMail IM Option on Symantec.cloud™ arbeitet mit unterstützten Instant Messaging-Netzwerken und -Clients zusammen. Aktuell gehören dazu öffentliche Instant Messaging-Netzwerke wie AOL, MSN, Yahoo und Google Talk, private Netzwerke (Reuters) und Instant Messaging-Clients in Unternehmensumgebungen (Microsoft Office Communicator, Lotus Sametime und Jabber).
1.5.2 Instant Messages werden indiziert und in ihrer ursprünglichen Form auf Medien kopiert, auf denen sie dann durchsucht werden können.
1.5.3 Der Kunde kann Instant Messaging-Gespräche anhand verschiedenster Suchkriterien wie Datumsbereich, Schlüsselwort oder Ausdruck und Sender/Empfänger durchsuchen und abrufen.
1.5.4 Zu Prüfzwecken wird ein Verlaufsprotokoll erstellt.

1.6 AdvisorMail Bloomberg Option on Symantec.cloud™
AdvisorMail Bloomberg Option on Symantec.cloud™ ist der internetbasierte Archivierungsservice von Symantec für Instant Bloomberg (Instant Messages) und Bloomberg-E-Mail. Bloomberg-Nachrichten werden in Advisor Mail aufgezeichnet, gespeichert und indiziert und dann in Übereinstimmung mit den Richtlinien des Unternehmens überwacht. Bloomberg-Nachrichten, die bestimmte Schlüsselwörter oder Ausdrücke enthalten, können dann von Compliance-Mitarbeitern geprüft werden. AdvisorMail Bloomberg Option on Symantec.cloud™ kann als zusätzlicher Service optional zu Advisor Mail hinzugekauft werden
1.6.1 Der AdvisorMail Bloomberg Option on Symantec.cloud™-Service zeichnet Instant Bloomberg-Nachrichten und Bloomberg-E-Mail in Advisor Mail in ihrem systemeigenen Format auf.
1.6.2 Bloomberg-Nachrichten werden indiziert und in ihrer ursprünglichen Form auf Speichermedien kopiert, auf denen sie dann durchsucht werden können.
1.6.3 Der Kunde kann Bloomberg-Nachrichten anhand verschiedenster Suchkriterien wie Datumsbereich, Schlüsselwort oder Ausdruck und Sender/Empfänger durchsuchen und abrufen.
1.6.4 Zu Prüfzwecken wird ein Verlaufsprotokoll erstellt.

1.7 Reserviert

1.8 Symantec Enterprise Vault.cloud Data Import Option

Der internetbasierte Symantec Enterprise Vault.cloud Data Import Option migriert und integriert vorhandene E-Mail-Legacy-Daten in das Archiv-Repository des Kunden. Mit dem Importdienst kann der Kunde dann sein E-Mail-Archiv (z. B. persönliches Archiv, Discovery-Archiv und Advisor Mail), einschließlich integrierter Legacy-E-Mail und neuer E-Mail-Ströme, durchsuchen.

1.8.1 Für den Symantec Enterprise Vault.cloud Data Import Option müssen Kunden E-Mail-Daten via S-FTP oder sicherem Kurier im PST- oder EML-Dateiformat senden.

1.8.2 Der Kunde kann die Daten manuell extrahieren und im PST- oder EML-Format bereitstellen.

1.8.3 In Übereinstimmung mit den Richtlinien des Kunden weist Symantec Enterprise Vault.cloud Data Import Option jeder gefundenen Nachricht Besitzrechte zu. Nachrichten, die keiner bestimmten Person direkt zugewiesen werden können, werden in einer "Auffang"-Mailbox im E-Mail-Archiv archiviert.

1.8.4 Alle Migrationsaktivitäten können protokolliert und geprüft werden, um Informationsintegrität in den E-Mail-Datensätzen des Kunden herzustellen und die "Obhutskette" (Chain of Custody) zu bewahren.

1.8.5 Der Symantec Enterprise Vault.cloud Data Import Option erfordert die aktive Mitarbeit des Kunden bei der Planung, Analyse und Ausführung eines Integrationsplans, der Störungen des Geschäftsbetriebs weitgehend vermeidet.

1.8.6 Die maximale Größe von E-Mails, die aufgenommen werden können, beträgt 40 MB.

1.9 Symantec Enterprise Vault Mailbox Continuity.cloud

FALLS SYMANTEC KEINE SMTP-VERBINDUNG MIT DEM KUNDEN HERSTELLEN KANN, WERDEN DIE E-MAILS DES KUNDEN IM AUFTRAG DES KUNDEN AUF DEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD SERVICE UMGELEITET ("CONTINUITY-EREIGNIS"). UM ALLE ZWEIFEL AUSZUSCHLIESSEN: (I) WENN DIE FIREWALL DES KUNDEN DIE FUNKTION EINES PROXY ÜBERNIMMT UND ANSTELLE DES E-MAIL-SERVERS ANTWORTET ODER (II) WENN DER E-MAIL-SERVER DES KUNDEN EINE ANTWORT AUSGIBT (EINSCHLIESSLICH, OHNE DARAUF BESCHRÄNKT ZU SEIN, FEHLERCODES), DANN GILT DIES ALS EINE SMTP-VERBINDUNG UND WIRD NICHT ALS CONTINUITY-EREIGNIS GEWERTET.

1.9.1 Während eines Continuity-Ereignisses können die jeweiligen Benutzer des Kunden über einen speziell eingerichteten Ordner in Microsoft Outlook® oder eine webbasierte Benutzeroberfläche auf ihre E-Mails zugreifen. Benutzer können: (i) auf bis zu neunzig (90) Tage alte E-Mails zugreifen, einschließlich den während des Continuity-Ereignisses gesendeten und empfangenen neuen E-Mails; (ii) E-Mails verfassen, beantworten und weiterleiten; und (iii) gängige E-Mail-Funktionen wie Rechtschreibprüfung, Einfügen von Anhängen und Formatieren verwenden.

1.9.2 Falls der Kunde nur Symantec Enterprise Vault Mailbox Continuity.cloud abonniert hat, werden Continuity-E-Mails in diesem Service neunzig (90) Tage lang gespeichert. Falls der Kunde unter diesem Anhang 17 einen weiteren Archivierungsservice erworben hat, werden Continuity-E-Mails so lange aufbewahrt, wie vom Kunden in diesem Service ausgewählt.

1.9.3 Continuity-E-Mails werden an den Primärserver des Kunden zu dem Zeitpunkt zugestellt, zu dem dieser Server E-Mails wieder akzeptiert. Von dieser Zustellung ausgenommen sind E-Mails, die bereits länger als sieben (7) Tage in der Warteschlange waren. Der Kunde muss diese E-Mails aus dem Continuity-Archiv wie oben in Klausel 1.9.2 beschrieben abrufen.

1.9.4 Der Symantec Enterprise Vault Mailbox Continuity.cloud Service verwendet eine opportunistische anstelle einer erzwungenen Transport Layer Security ("TLS")-Verbindung bei der E-Mail-Zustellung. TLS ist ein erweitertes Sicherheitsprotokoll, das E-Mail während der Übertragung über das Internet schützt/verschlüsselt. **SÄMTLICHE BOUNDARY ENCRYPTION- UND POLICY BASED ENCRYPTION-KUNDEN, DIE ZUSÄTZLICH DEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD SERVICE ABONNIEREN, BESTÄTIGEN UND STIMMEN ZU, DASS VERSUCHT WIRD, EINE TLS-VERBINDUNG HERZUSTELLEN, EINE HERSTELLUNG EINER SOLCHEN VERBINDUNG JEDOCH GGF. NICHT MÖGLICH IST UND E-MAILS AUS DIESEM GRUND EVENTUELL NICHT VERSCHLÜSSELT WERDEN**. **DEMENTSPRECHEND ERKENNT DER KUNDE AN, DASS ER/SIE KEINE VERTRAULICHEN E-MAILS ÜBER DEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD SERVICE SENDEN ODER EMPFANGEN SOLLTE UND EIN SENDEN BZW. EMPFANGEN SOLCHER E-MAILS AUSSCHLIESSLICH AUF EIGENES RISIKO DES KUNDEN ERFOLGT.**

1.9.5 Symantec Enterprise Vault Mailbox Continuity.cloud-Pflichten

Der Symantec Enterprise Vault Mailbox Continuity.cloud Service stellt E-Mails nur an einen einzelnen benannten Server pro definierter Domäne und "pro Benutzer-Routing" zu. Kunden stimmen hiermit diesem Aspekt des Service zu. Der Kunde stimmt zu, den Symantec Enterprise Vault Mailbox Continuity.cloud Service als Failover-Zustellungskanal mit der ClientNet-Schnittstelle zu konfigurieren und ferner Symantec den Zustellungsort (Mailhost-Name oder IP-Adresse) nach Domäne seiner E-Mail-Server zu Beginn dieses Service mitzuteilen. Der Kunde bestätigt und stimmt zu, dass es seine Pflicht ist, Symantec während der Laufzeit des Symantec Enterprise Vault Mailbox Continuity.cloud Service über Änderungen dieses Zustellungskanals zu informieren. Der Kunde bestätigt, dass das Unvermögen des Kunden, diese Konfigurationen durchzuführen oder diese Zustellinformationen an Symantec weiterzuleiten, negative Auswirkungen auf die Funktionsfähigkeit des Symantec Enterprise Vault Mailbox Continuity.cloud Service hat.

1.10 Symantec Enterprise Vault.cloud Folder Sync Option

1.10.1 Der Symantec Enterprise Vault.cloud Folder Sync Option ist ein Zusatzservice zum Enterprise Vault Personal.cloud Service, der ausschließlich in Abschnitt 1.1 dieses Anhangs beschrieben wird. Mithilfe des Symantec Enterprise Vault.cloud Folder Sync Option kann ein Kunde seine E-Mails im Symantec Enterprise Vault Personal.cloud Service ähnlich wie in der E-Mail-Struktur der Outlook-Ordner des Kunden anzeigen. Mithilfe des Symantec Enterprise Vault.cloud Folder Sync Option können Administratoren die Outlook-Ordnerstruktur des Kunden innerhalb von Symantec Enterprise Vault Personal.cloud synchronisieren. Wenn Kunden E-Mail-Nachrichten zwischen Outlook-Ordnern verschieben und neue Outlook-Ordner erstellen bzw. den Speicherort von Outlook-Ordnern ändern, repliziert der Synchronisierungsservice anschließend diese Struktur in Symantec Enterprise Vault Personal.cloud.

1.10.2 Symantec Enterprise Vault.cloud Folder Sync Option wird von Administratoren für den Kunden über einen lokalen Service bereitgestellt, der Verschiebungen von Ordnern und Ordnerelementen aufzeichnet.

1.10.3 Nach der Erstsynchronisierung führt Symantec Enterprise Vault.cloud Folder Sync Option inkrementelle Synchronisierungen zwischen Outlook-Ordnern und Symantec Enterprise Vault Personal.cloud durch.

1.10.4 Inkrementelle Synchronisierungen können nach Zeitplan stündlich, täglich oder wöchentlich durchgeführt werden. Das Synchronisierungsintervall wird vom Kunden festgelegt.

1.10.5 Ein Kunde kann die Ergebnisse einer Archivsuche filtern, indem er die Filterfunktion aktiviert und einen Ordner in der von den Suchfiltern zurückgegebenen Liste auswählt.

1.10.6 Der Service wird nur auf Microsoft Exchange Server 2003-, 2007- oder 2010-Plattformen unterstützt.

2. Zusatzvereinbarungen.

2.1 Symantec weist darauf hin, dass die Konfiguration und Verwendung des Service allein der Kontrolle des Kunden unterliegt. Symantec empfiehlt Kunden, Nutzungsbedingungen für Computer (oder vergleichbare Richtlinien) aufzustellen. In bestimmten Ländern muss gegebenenfalls die Zustimmung einzelner Mitarbeiter eingeholt werden. Symantec empfiehlt Kunden, vor Bereitstellung des Service stets sicherzustellen, dass örtlich geltende Gesetze und Bestimmungen eingehalten werden. Symantec übernimmt keine Verantwortung für die zivilrechtliche oder strafrechtliche Haftung, die der Betrieb des Service nach sich ziehen kann.
2.2 **DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN USA ERBRACHT WERDEN UND ES AUFGABE DES KUNDEN IST, ALLE ZUSTIMMUNGEN UND GENEHMIGUNGEN ZU EINZUHOLEN, DIE ERFORDERLICH SIND, UM DEN TRANSFER VON DATEN ZU VERANLASSEN. DER KUNDE BESTÄTIGT UND STIMMT DES WEITEREN ZU, DASS SYMANTEC KEINE VERANTWORTUNG FÜR VERSTÖSSE GEGEN GELTENDE BESTIMMUNGEN ODER GESETZE ÜBERNIMMT.**
2.3 Der Kunde bestätigt und stimmt zu, dass (i) die Scanservices von Symantec (Email AV, Email AS, Email IC und Email CC) nicht alle E-Mail-Nachrichten scannen, die ursprünglich dem Archiv zugestellt wurden, und (ii) dass die Scanservices von Symantec (Email AV, Email AS, Email IC und Email CC) keine E-Mails scannen, die aus dem Archiv zur Wiederinkraftsetzung in der Mailbox eines Benutzers freigegeben wurden. Dementsprechend übernimmt Symantec keine Haftung für Viren, Spam, Bilder oder ungeeignete Inhalte, die in solchen wiederhergestellten E-Mails enthalten sein können. Darüber hinaus findet die Service Level-Vereinbarung auf diese wiederhergestellten E-Mails keine Anwendung.
2.4 Vorbehaltlich der Bestimmungen und Bedingungen dieser Vereinbarung gewährt Symantec dem Kunden das nicht ausschließliche, nicht übertragbare Recht zur Installation und Nutzung einer jeden Software im Rahmen der oben genannten Services und nur soweit dies für den internen Unternehmensbetrieb des Kunden erforderlich ist. Alle Rechte an geistigem Eigentum in dieser Software sind und bleiben im Besitz von Symantec (und/oder deren Zulieferer). Diese Software wird nicht verkauft, sondern von Symantec lizenziert. Der Kunde bestätigt, dass die Software und sämtliche zugehörigen Informationen, einschließlich und uneingeschränkt aller Updates, Eigentum von Symantec und ihrer Zulieferer ist. Der Kunde übernimmt die Verantwortung und haftet uneingeschränkt für die Einhaltung oder die Verletzung der Bestimmungen dieser Vereinbarung durch jeden einzelnen Benutzer. Der Kunde verpflichtet sich, Symantec von jeder nicht autorisierten Nutzung dieser Lizenz oder einem Verstoß gegen Bestimmungen dieser Lizenz zu informieren.
2.5 Der Kunde bestätigt und stimmt zu, dass Symantec unter keinen Umständen die Funktion eines Drittanbieter-Downloaders im Sinne der SEC-Bestimmungen übernehmen kann.
2.6 Sämtliche von Symantec oder seinen Drittanbietern im Rahmen dieser Vereinbarung gespeicherten oder archivierten Kundendaten sind alleiniges Eigentum des Kunden ("Kundendaten"). Keine der in diesem Dokument enthaltenen Bestimmungen überträgt Symantec oder seinen Anbietern irgendwelche gesetzlichen oder billigkeitsrechtlichen Rechte, Titel oder Interessensansprüche an den Kundendaten.
2.7 Die Kundendaten werden während der Laufzeit des Service sowie für einen Zeitraum von hundertzwanzig (120) Tagen nach Laufzeitende des Service oder hundertzwanzig (120) Tagen nach dem Ablaufdatum, falls der Service vor dem Laufzeitende beendet wird (zusammenfassend als "Aufbewahrungszeitraum nach Ablauf" bezeichnet), gespeichert oder archiviert. Während oder vor dem Aufbewahrungszeitraum nach Ablauf kann der Kunde Symantec schriftlich auffordern: (i) die Kundendaten zu löschen, ohne dass zusätzliche Kosten anfallen (falls eine Löschung nicht per Gesetz oder Gerichtsbeschluss verboten ist); oder (ii) dem Kunden eine Offline-Kopie im PST-Format auf Festplatte zuzustellen, wobei hierfür die zu diesem Zeitpunkt gültigen Gebühren von Symantec gelten und eine Zustellung von maximal zwei (2) Terabyte pro Monat so lange erfolgt, bis sämtliche Kundendaten an den Kunden geliefert wurden. Falls der Kunde Symantec keine wie im vorangehenden Satz beschriebene schriftliche Anweisung zukommen lässt, ist Symantec berechtigt, die Kundendaten am Ende des Aufbewahrungszeitraums nach Ablauf zu löschen (falls eine Löschung nicht per Gesetz oder Gerichtsbeschluss verboten ist).

Q – Symantec Endpoint Protection.cloud

1. Überblick

1.1 Zum Bezug des Symantec Endpoint Protection.cloud Service muss der Kunde einen Agenten auf den betreffenden Benutzercomputern installieren und eine entsprechende Richtlinie für die Nutzung des Service zuweisen. Das Verwaltungsportal des Hosted Endpoint Protection-Service ist ein Administrator-Portal für die Verwaltung von Computern, Richtlinien, Warnmeldungen und Berichten ("Verwaltungsportal").
1.2 Der Kunde muss ggf. einige einfache Firewall-Änderungen vornehmen, damit der Agent mit der Symantec Hosted Services-Infrastruktur kommunizieren und zusammenarbeiten kann.
1.3 Sobald der Service gemäß Absatz 1.1 und 1.2 konfiguriert wurde, wird das Verwaltungsportal für die Verwaltung des/der Agenten verwendet.
1.4 Symantec veröffentlicht eine Liste der unterstützten Computerbetriebssysteme für den Agenten sowie der unterstützten Browser für das Verwaltungsportal. Der Kunde erkennt an und stimmt zu, dass Symantec diese Liste regelmäßig und ohne vorherige Ankündigung aktualisieren und ändern kann.
1.5 Der auf dem Computer installierte Agent:
1.5.1 Soll den Computer vor erkannter Malware basierend auf bekannten Methoden entsprechend dem jeweiligen Service schützen
1.5.2 Soll bekannte bösartige Angriffe aus dem Netzwerk auf den Computer blockieren
1.5.3 Soll Antiphishing-Funktionen in den unterstützten Browsern bereitstellen, die als Phishing eingestufte Angriffe abwehren

2. Verwaltungsportal

2.1 Mithilfe des Verwaltungsportals kann der Kunde seine eigenen richtlinienbasierten Sicherheitmaßnahmen für die Agenten konfigurieren.
2.2 Der Kunde ist dafür verantwortlich, die Konfigurationsoptionen in Übereinstimmung mit der vom Kunden festgelegten Computernutzungsrichtlinie (oder einer gleichwertigen Richtlinie) über das Verwaltungsportal zu implementieren. Richtlinien werden für die Computergruppe konfiguriert.
2.3 Für die Richtlinie vorgenommene Änderungen werden umgehend im Verwaltungsportal angezeigt und im Stapelmodus an die Agenten verteilt. Aktuelle Richtlinieneinstellungen in einzelnen Agenten können im Verwaltungsportal oder in dem Agenten, der auf dem Benutzercomputer ausgeführt wird, angezeigt werden.

3. Protokolle und Berichte

3.1 Sämtliche vom Agenten erstellten Protokolle und Berichte werden für einen Zeitraum von zwölf (12) Monaten im Verwaltungsportal gespeichert und können innerhalb dieses Zeitraums im Verwaltungsportal angezeigt und heruntergeladen werden. Nach dieser Frist werden die Protokolle gelöscht.

4. Benachrichtigungen

4.1 Der Kunden kann den Hosted Endpoint Protection-Service so konfigurieren, dass eine automatische Benachrichtigung an konfigurierte E-Mail-Empfänger basierend auf der im Verwaltungsportal konfigurierbaren Benachrichtigungsregel gesendet wird.
4.2 Der Kunde kann Benachrichtigungen im Verwaltungsportal erstellen, löschen und anpassen.

5. Support

5.1 Zu den Supportleistungen gehören:
5.1.1 Führung durch das Verwaltungsportal, einschließlich einer Servicebeschreibung sowie einer Frage- und Antwortsitzung. (Dies schließt <u>keine</u> Hilfestellung bei der Einrichtung von Richtlinien oder Analyse der Wirksamkeit der Richtlinien ein.)
5.1.2 Administratorhandbuch
5.1.3. Benutzerhandbuch

6. Datenschutz im Zusammenhang mit Hosted Endpoint Protection

6.1 Der Kunde erkennt an, dass die Protokolle personenbezogene Daten enthalten können und die Protokollierung sowie das Abfangen von Protokollen daher eine Verarbeitung persönlicher Daten darstellen kann. Des Weiteren erkennt der Kunde an, dass Hosted Endpoint Protection ein konfigurierbarer Service ist und der Kunde die alleinige Verantwortung für die Konfiguration des Hosted Endpoint Protection-Service in Übereinstimmung mit der vom Kunden festgelegten Computernutzungsrichtlinie (oder einer gleichwertigen Richtlinie) sowie sämtlicher geltenden Gesetze oder Vorschriften übernimmt. Dementsprechend weist Symantec Symantec Hosted Services den Kunden darauf hin, vor der Implementierung von Hosted Endpoint Protection örtlich geltende Gesetze zu überprüfen und sicherzustellen, dass der Kunde sowie sämtliche Mitarbeiter des Kunden die Pflichten kennen und einhalten, denen sie in Bezug auf Datenschutzgesetze und/oder -vorschriften bei der Verwendung von Hosted Endpoint Protection durch den Kunden unterliegen. In bestimmten Ländern muss gegebenenfalls die Zustimmung einzelner Mitarbeiter vor der Protokollierung und dem Abfangen von Protokollen eingeholt werden. Der Kunde ist verpflichtet jeden Hosted Endpoint Protection-Agenten mit angemessener und minimaler Anpassung zu installieren. Der Kunde erkennt an und stimmt zu, dass Geräte, die vom Hosted Endpoint Protection Service abgedeckt werden, (i) Informationen bezüglich des Betriebs der Hosted Endpoint Protection Services protokollieren, (ii) diese Informationen an Symantec zum Zweck der Bereitstellung von Verwaltungsinformationen und Berichten an den Kunden überträgt und (iii) dass der Kunde diese Protollierung und Übertragung genehmigt. Symantec Symantec Hosted Services übernimmt keine Verantwortung für die zivilrechtliche oder strafrechtliche Haftung, die der Betrieb des Hosted Endpoint Protection-Service durch den Kunden nach sich ziehen kann.
6.2 **DER KUNDE AKZEPTIERT UND STIMMT ZU, DASS DIE SERVICELEISTUNGEN TEILWEISE ODER GANZ IN DEN USA ERBRACHT WERDEN UND ES AUFGABE DES KUNDEN IST, ALLE ZUSTIMMUNGEN UND GENEHMIGUNGEN ZU EINZUHOLEN, DIE ERFORDERLICH SIND, UM DEN TRANSFER VON DATEN ZU VERANLASSEN. DER KUNDE BESTÄTIGT UND STIMMT DES WEITEREN ZU, DASS SYMANTEC KEINE VERANTWORTUNG FÜR VERSTÖSSE GEGEN GELTENDE BESTIMMUNGEN ODER GESETZE ÜBERNIMMT**.

7. Konfiguration

7.1 Falls der Kunde den Service über einen Symantec-Händler erworben hat, autorisiert der Kunde diesen Symantec-Händler ausdrücklich zur Ausführung folgender Aufgaben: (i) Ändern von Konfigurationseinstellungen des Service, um eine optimale Funktionsweise des Service zu erreichen, und (ii) Einreichen von Support-Tickets im Namen des Kunden.

R – Symantec MessageLabs Web v2 Smart Connect.cloud ("Smart Connect.cloud")

1. **Überblick**

1.1. Sobald der Agent für Roaming-Benutzer installiert ist und die erforderlichen Konfigurationsänderungen vorgenommen wurden, werden angeforderte Webseiten und Anhänge über den Benutzeragenten elektronisch an den Symantec MessageLabs Web v2 URL.cloud Service ("Web v2 URL") sowie an den Symantec MessageLabs Web v2 Protect.cloud Service ("Web v2 Protect") weitergeleitet und digital überprüft.

2. **Leistungsbeschreibung**

2.1. Wenn der Benutzer in vertraglich festgelegten "Serviceländern" auf das Internet zugreift, werden die externen HTTP- und FTP-over-HTTP-Anfragen des Kunden, einschließlich aller Anhänge, Makros oder ausführbaren Dateien, über die Web v2 URL- und Web v2 Protect-Services weitergeleitet.

3. **Konfiguration**

3.1. Die Konfigurationseinstellungen, die zur Umleitung dieses externen Internetdatenverkehrs an die Software des Agenten für Roaming-Benutzer sowie zur Weiterleitung des ausgehenden Datenverkehrs an die Web v2 URL-und Web v2 Protect-Services erforderlich sind, werden vom Kunden vorgenommen und verwaltet und sind von der technischen Infrastruktur des Kunden abhängig. Der Kunde muss eine PAC-Datei auf dem PC des Benutzers installieren, so dass der Browser beim Starten auf den Roaming-Agenten von Symantec verweist. Eine PAC-Dateivorlage kann aus ClientNet heruntergeladen und vom Kunden angepasst werden. Der Kunde muss sicherstellen, dass interner HTTP/FTP-over-HTTP-Datenverkehr (beispielsweise in das Unternehmensintranet) nicht an die Software für den Roaming-Agenten weitergeleitet wird.

3.2. Der Zugriff auf Web v2 URL und Web v2 Protect ist auf autorisierte Systeme, die über eine gültige Version der Software für den Roaming-Agenten des Kunden verfügen, sowie auf autorisierte Benutzer, die für diese Services im ClientNet aktiviert wurden, beschränkt. Der Roaming-Software-Agent und autorisierte Benutzerinformationen werden zur Identifizierung des Kunden und zur dynamischen Auswahl kundenspezifischer Einstellungen verwendet.

3.3. Die Richtlinienregeln für den Web v2 URL Service und die Content-Scans für den Web v2 Protect-Service gelten unabhängig davon, ob der Benutzer den Roaming-Agent-Service verwendet oder über ein konfiguriertes Netzwerkverzeichnis (d. h. ein Unternehmens-LAN) verbunden ist.

3.4. Der Kunde erkennt an, dass auf dem Roaming-Agenten von Beginn an die Symantec-Standardeinstellungen festgelegt sind. Dies schließt ein, dass die notwendigen Anstrengungen unternommen werden, um den Internetdatenverkehr des Benutzers zu einem "optimalen" Zugriffspunkt in der Serviceinfrastruktur weiterzuleiten. Diese Weiterleitung basiert auf der Ermittlung des Standorts des Roaming-Benutzers anhand einer IP-Adresse und der Verwendung einer Positionsdatenbank eines Drittanbieters zur Identifizierung des Landes, von dem aus der Benutzer zu dem betreffenden Zeitpunkt wahrscheinlich zugreift. Symantec leitet Benutzer mithilfe der zutreffenden Länderbezeichnung zu dem als optimal eingestuften Servicezugriffspunkt für das angegebene Land um. Dies geschieht unabhängig von einer Bewertung der wahrscheinlichen Leistung des Internetzugangs des Endbenutzers und erfolgt nur für diejenigen Länder, deren Servicequalität von Symantec als ausreichend erachtet wird.

Der Kunde erkennt an, dass Symantec für alle Länder außerhalb der geeigneten Serviceländer keine Web v2 URL- oder Web v2 Protect-Serviceleistungen bereitstellt. Wenn in solchen Situationen festgestellt wird, dass der Endbenutzer sich in einem Land befindet, bei dem es sich nicht um ein "Serviceland" handelt, wird der Roaming-Agent nicht geöffnet ("fail open"), so dass der Benutzer zwar auf das Internet zugreifen, die Vorteile der Symantec-Leistungen, die in akzeptablen Serviceländern verfügbar sind, jedoch nicht nutzen kann.

DER KUNDE BESTÄTIGT UND STIMMT ZU, DASS DER INTERNETDATENVERKEHR DES BENUTZERS ZUR VERARBEITUNG IN ÜBEREINSTIMMUNG MIT ABSATZ 3.4 DER VORLIEGENDEN VEREINBARUNG ZU EINER INFRASTRUKTUR UMGELEITET WERDEN KANN, DIE SICH IN EINEM LAND AUSSERHALB DER EU BEFINDET: ES IST AUFGABE DES KUNDEN, ALLE ZUSTIMMUNGEN UND GENEHMIGUNGEN EINZUHOLEN, DIE ERFORDERLICH SIND, UM DEN TRANSFER VON SOLCHEN INTERNETDATEN ZU VERANLASSEN. DER KUNDE BESTÄTIGT UND STIMMT DES WEITEREN ZU, DASS SYMANTEC KEINE VERANTWORTUNG FÜR VERSTÖSSE GEGEN GELTENDE BESTIMMUNGEN ODER GESETZE ÜBERNIMMT.

4. **Zusätzliche Exportvereinbarungen für Smart Connect**

4.1 Kunden oder Partner sind nicht berechtigt und dürfen Dritte nicht autorisieren, die Kontrollgesetzen unterliegende Technologie direkt oder indirekt in eines der folgenden Länder zu verkaufen, weiterzuveräußern, zu exportieren, wiedereinzuführen ("re-exportieren"), zu übertragen, umzuleiten, zu verteilen, zu entsorgen, offenzulegen oder anderweitig dort in Umlauf zu bringen: Afghanistan, Angola, Armenien, Aserbaidschan, Bosnien und Herzegowina, Burma, Burundi, China, Kuba, Demokratische Republik Kongo, Eritrea, Äthiopien, Iran, Irak, Nordkorea, Liberia, Libyen, Nigeria, Ruanda, Sierra Leone, Somalia, Sudan, Syrien, Tansania, Uganda und Zimbabwe.

4.2 Kunden oder Partner sind nicht berechtigt, den Web Roaming Agent auf ein anderes Unternehmen oder eine andere Einzelperson, die kein Mitarbeiter des Kunden oder Partners ist, zu übertragen. Dazu gelten folgende Ausnahmen: (i) Kunden oder Partner sind berechtigt, den Web Roaming Agent zur Nutzung im Auftrag des Kunden oder des Partners auf ihre Vertragspartner zu übertragen oder das Herunterladen des Web Roaming Agent durch ihre Vertragspartner zu dem vorgenannten Zweck zu ermöglichen; und oder (ii) der Kunde oder Partner ist berechtigt, den Web Roaming Agent an seine Endkunden, an die er den Symantec Service verkauft, zu übertragen bzw. den Download des Web Roaming Agent durch seine Endkunden, an die er den Symantec Service verkauft, zu ermöglichen, vorausgesetzt, dass der Kunde oder Partner solche Drittanbieter über deren Verpflichtungen in Bezug auf diesen Abschnitt unterrichtet.