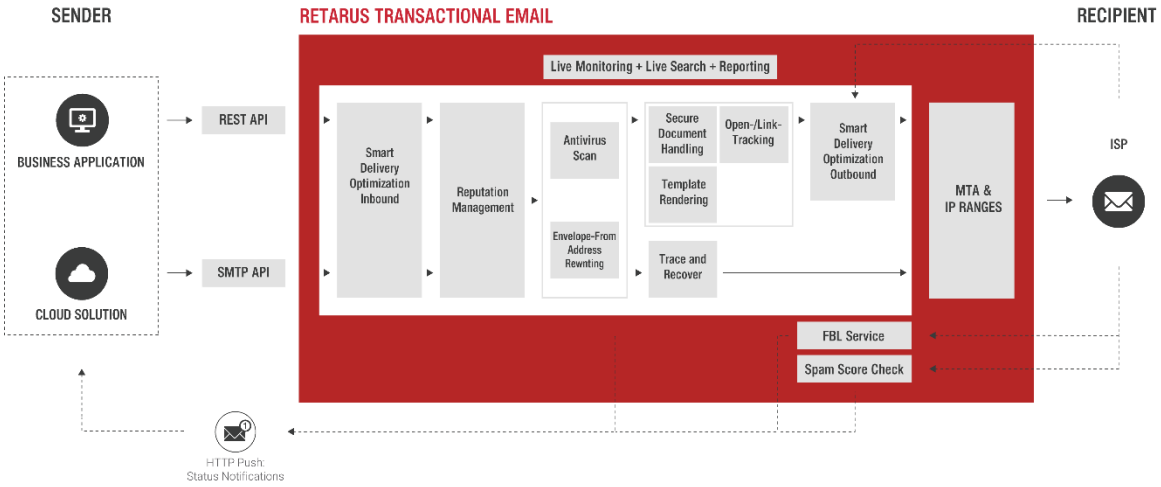
Service-Beschreibung und Mitwirkungspflichten
Retarus Transactional Email

Mit **Retarus Transactional Email** lassen sich große Email-Volumina direkt aus Geschäftsanwendungen ohne Belastung der eigenen Email-Infrastruktur versenden. Dazu wird die Kundeninfrastruktur über etablierte Schnittstellen an das Global Delivery Network von Retarus angeschlossen. Die Datenverarbeitung erfolgt in Retarus-eigenen Rechenzentren.

Inhalt

Systemarchitektur Retarus Transactional Email



Schnittstellen

SCHNITTSTELLEN	REST (V2)	SMTP
Max. Versandvolumen pro Stunde	Nach Anforderung skalierbar	Nach Anforderung skalierbar
Smart Delivery Optimization	✓	✓
Status-Informationen jeder Email	API-Callback (Webhooks)	API-Callback (Webhooks)
Email Reporting (CSV)	✓	✓
Smart Network Data Services Reporting*	Auf Anfrage	Auf Anfrage
Reputation Management	• Dedizierte IP (optional) • Blacklist-Monitoring • Live-Monitoring • SPF / DKIM • Suppression List • Registered Sender Domain • Feedback Loop Service* • CSA-zertifiziert* (EU, CH) • IPv6-/IPv4-Support	• Dedizierte IP (optional) • Blacklist-Monitoring • Live-Monitoring • SPF / DKIM • Suppression List • Registered Sender Domain • Feedback Loop Service* • CSA-zertifiziert* (EU, CH) • IPv6-/IPv4-Support
List Unsubscribe Header Unterstützung	✓	✓
Mandantenfähig (Multi-Domain-Konfiguration)	✓	✓
IP-Whitelisting	✓	✓
Verschlüsselte Anbindung an Retarus Global Delivery Network	✓	✓
Technische Voraussetzungen	HTTPS-API-Client (Job) und empfangender Webservice (Status)	Anwendung mit SMTP-Unterstützung (Job) und empfangender Webservice (Status)
Open Tracking	✓	-
Link Tracking	✓	-
Envelope-From Address Rewriting	✓	✓
Outbound AntiVirus MultiScan	✓	✓
Secure Document Handling	✓	-
Template-Rendering	✓	-
Trace & Recover	-	✓
Spam Score Check	✓	✓
EAS Live Monitoring	✓	✓
EAS Live Search	✓	✓
EAS Reporting	✓	✓
Max. Mailgröße	20 MB	20 MB

Basiskonfiguration

Die Basiskonfiguration beinhaltet Zugangsdaten bzw. eine registrierte Authentification-IP zu einem API-Endpoint oder zu einem SMTP-Server in einem Retarus-Rechenzentrum. Die Kommunikation erfolgt über eine sichere Verbindung via HTTPS und/oder SMTP Auth Basic via eTLS. Die Einrichtung umfasst eine Sender-Domain pro IPv6-Adresse*, Default-Job-Parameter, IP-Routing, SPF-Record und DKIM-Signatur. Der Account wird nach vollständiger Einrichtung der beauftragten Pakete freigeschaltet. Retarus stellt eine Schnittstellenbeschreibung bereit.

*Erläuterung IPv6-Adresse: Die Nutzung nachfolgender Funktionalitäten innerhalb der Services erfordern die Nutzung von IPv4-Adressen:

- Smart Network Data Services Reporting
- Feedback Loop Service
- CSA-zertifizierte IP-Bereiche (Certified Senders Alliance)

Dedicated IP

Einer oder mehreren Sender-Domains werden dedizierten IP-Adressen zugeordnet. Hierdurch kann z. B. die Email-Kommunikation aus unterschiedlichen Anwendungen oder von Mutter-/Tochter-Unternehmen getrennt werden. Die Nutzung von dedizierten IP-Adressen (Dedicated IPs) wird ab einem Volumen von 1.000.000 Emails pro Monat empfohlen. Da der Transactional Email Service i.d.R. in einem Rechenzentrumsverbund (Active/Active) genutzt wird, setzt die Nutzung von Dedicated IPs eine Mindestanzahl von zwei dedizierten IP-Adressen voraus. Mit der Einrichtung von dedizierten IP-Adressen, werden dem Kunden für die Dauer der Vertragslaufzeit durch Retarus IP-Adressen zur Nutzung überlassen. Diese werden in das Blacklist-Überwachungssystem von Retarus integriert. Ein Austausch der IP-Adresse durch Retarus ist jederzeit möglich.

Enforced TLS

Auf Ebene der Versand-Domäne wird während der Basiskonfiguration des Dienstes festgelegt, ob ein hybrides Verschlüsselungsprotokoll für jeden Versand angewandt werden soll. Damit wird eine verschlüsselte Verbindung aufgebaut, wenn der Kunde über die vorgegeben Domäne Emails versendet (enforced TLS). Falls die Empfängerseite keine verschlüsselte Verbindung akzeptiert, wird der Versand abgebrochen.

Envelope-From Address Rewriting

Optional bietet Retarus die Möglichkeit, die Envelope-From-Adresse des Kunden für ausgehende Emails umzuschreiben. Damit lassen sich mögliche Antworten auf ein dediziertes Postfach umleiten. Das Umschreiben von Adressen ist besonders nützlich, wenn es z. B. aus unternehmerischen Richtlinien nicht erlaubt ist, mit der hauseigenen Domain Nachrichten via Internet zu versenden.

Smart Delivery Optimization

Retarus steuert den Versand und den Empfang von Emails via Smart Delivery Optimization. Das ermöglicht es, einen möglichst hohen Durchsatz bei ISPs und ESPs aufrecht zu erhalten. Dafür passt Smart Delivery Optimization das Sendeverhalten des Kunden automatisiert an die Rückmeldungen einzelner ISPs und/oder ESPs an. Die optimierte Versandsteuerung kann zu einer Verringerung der vereinbarten Verarbeitungskapazität führen.

Statusinformationen via API-Callback (Webhook)

Retarus stellt Statusinformationen via API-Callback (Webhook) zu Verfügung. Zu neu erzeugten Events wird der Kunde informiert, z. B. über den Zustellungsstatus, Gründe für Unzustellbarkeiten, Blockieren von Emails an Empfänger, die in der Suppression List verzeichnet sind, und Informationen zu Open- und Link-Tracking. Via http-Post lassen sich diese Statusinformationen automatisiert in Geschäftsprozesse und Applikationen integrieren. Damit unterstützt Retarus die Pflege der Stammdaten (Database Hygiene) sowie das aktive Bounce- und Traffic Management des Kunden und fördert somit die Reputation der kundeneigenen Domänen nachhaltig.

Retarus EAS (Enterprise Administration Services) – Live Monitoring

Retarus stellt im EAS-Portal ein Live-Monitoring zur Verfügung, anhand diesem in Real-Time versendete Emails verfolgt werden können. Diese Lösung ermöglicht es, Trendentwicklungen in den Bereichen Zustellung, Soft-/Hard-Bounces und Dropped Messages zu erkennen, um entsprechende Gegenmaßnahmen einleiten zu können.

Retarus EAS Live Search

Retarus stellt im EAS-Portal eine Live Search zur Verfügung. Die Suchfunktion bietet eine transparente Übersicht über alle vom Kunden versendeten Emails. EAS Live Search ermöglicht es, ausgehende Emails anhand von Zeiträumen, Message-IDs sowie Sendern und Empfängern zu suchen und dazu detaillierte Statusinformationen der letzten 45 Tage abzurufen.

Retarus EAS – Reporting

Retarus stellt im EAS-Portal ein Reporting zur Verfügung. Es bietet eine transparente Übersicht aller vom Kunden in den jeweils zurückliegenden 45 Tagen versendeten Emails, die im CSV- oder Excel-Format (XLSX) heruntergeladen werden kann.

Smart Network Data Service – Report (SNDS)

Der Smart Network Data Services (SNDS) Report listet in Form einer CSV-Datei detaillierte Daten zu vom Kunden genutzten IP-Adressen auf. Anhand dieser Daten kann der Kunde deren Reputation bei Microsoft besser nachvollziehen und verbessern. Dieser Service kann nur in Kombination mit einer dedizierten IP-Adresse genutzt werden.

Email Reporting (CSV)

Retarus stellt im EAS-Portal einen Versandreport im CSV-Format zur Verfügung. Dem Kunden stehen täglich aktualisierte Reports für insgesamt 180 Tage zum Abruf zur Verfügung. Die Reports erfassen nur Transaktionen, die einen finalen Status aufweisen. Transaktionen, die sich in der Verarbeitung befinden, werden nicht aufgeführt. Reports können in mehrere Teildateien aufgeteilt und komprimiert (z. B. im ZIP-Format) abgerufen werden.

Hinweis: Die Einrichtung eines CSV-Reports bedingt die temporäre Datenspeicherung zum Zweck der Leistungserfüllung. Die gespeicherten Daten enthalten Informationen über die Nachrichtenverarbeitung sowie personenbezogene Daten, z. B. Email-Adressen von Absendern und Empfängern, jedoch keine Inhaltsdaten.

Retarus Spam Score Check

Mit welcher Wahrscheinlichkeit Nachrichten als Spam eingestuft werden, hängt von mehreren Faktoren ab. Auslöser für Spam-Warnungen können ungewöhnliche HTML-Formatierungen oder Tabellenkonstruktionen, übermäßig viele Links oder unseriöse Formulierungen in Betreffzeile und Email-Body sein. Retarus stellt in diesem Zusammenhang den kostenpflichtigen Service „Spam Score Check“ als buchbare Option zu Verfügung. Mit diesem lässt sich vor der Aussendung prüfen, mit welcher Wahrscheinlichkeit eine Email als Spam eingestuft wird. Die Rückführung der Spam Scores erfolgt in einem automatisierten Verfahren, in dem die ermittelten Informationen von Retarus per Email an die zur Verfügung stehende Reply-To-Adresse des Kunden oder via API-Callback an einen bereitstehenden Webservice des Kunden zurückübermittelt. Nach erfolgreicher Übertragung werden alle Informationen zu dieser Sendung gelöscht und nicht archiviert.

Open- und Link-Tracking (optional CNAME)

Open-Tracking gibt die Öffnungsrate von Emails an, Link-Tracking erfasst die Öffnungsrate von in Emails erhaltenen Links. Dazu werden der Email-Body bzw. der Link so verändert, dass sich die Nachrichten auswerten lassen. Um die Wahrscheinlichkeit einer Spam-Klassifizierung zu reduzieren, empfiehlt Retarus, die kostenpflichtige Option CNAME zu buchen. Damit kann der Kunde eine eigene (Sub-) Domain verwenden. Hierbei setzt der Kunde einen A-Record der entsprechenden (Sub-) Domain auf eine Server-Adresse von Retarus. Der Kunde ist verpflichtet, die jeweiligen Email-Empfänger über das Open- und Link-Tracking über ausreichende Datenschutzerklärungen zu informieren und bei diesen gegebenenfalls die vorherige Zustimmung gemäß geltendem Recht einzuholen.

AntiVirus MultiScan

Retarus überprüft Nachrichten beim Versand auf Virenbefall. Dabei kann der Kunde selbst im Vorfeld bestimmen, ob nur die Anhänge einer Nachricht, und/oder der Nachrichtentext (Email-Body) auf Schadsoftware geprüft werden soll. Die Überprüfung erfolgt mit zwei Virenscannern verschiedener Anbieter nach Wahl von Retarus. Sobald diese Anbieter Updates oder neue Releases bereitstellen, wird Retarus diese schnellstmöglich zur Virenüberprüfung verwenden. Sofern ein Virenbefall festgestellt wird, löscht Retarus die entsprechende Nachricht. Statusinformationen über infizierte Emails werden dem Kunden per API-Callback (Webhook) übermittelt.

Secure Document Handling

Mit Secure Document Handling lassen sich Dateianhänge zu versendender Emails verschlüsseln. Zu diesem Zweck werden die Anhänge vor dem Versand in der Retarus-Infrastruktur automatisiert in ein ZIP-Archiv gepackt, das passwortgeschützt verschlüsselt wird. Die Passwörter stellt Retarus den Empfängern der betreffenden Emails separat zu. Um den höchstmöglichen Schutz zu erzielen, ist dieser Service nur in Kombination mit dem Retarus Outbound AntiVirus MultiScan erhältlich.

Trace & Recover

Die Funktion ermöglicht es, Emails die mittels einer SMTP-Anbindung übertragen werden, als Trace-&-Recover-Nachricht zu kennzeichnen. Alle für Trace & Recover gekennzeichneten Nachrichten werden 45 Tage lang in einem Kurzzeitspeicher abgelegt und sind in die Suchfunktion „Retarus EAS Live Search“ gefunden werden. Für die betroffene Nachricht steht eine Vorschau der ersten 1000

Satzzeichen zur Verfügung. Bevor die Nachricht bei Bedarf erneut versendet wird, kann nur der ursprüngliche Empfänger editiert werden.

Die Zusatzfunktion Trace & Recover setzt die Nutzung von AntiVirus MultiScan voraus und wird von Retarus für einen vom Kunden zu bestimmenden technischen Account aktiviert. Trace & Recover kann nicht im Zusammenhang mit Envelope-From Address Rewriting (Outbound) verwendet werden.

Verarbeitungskapazität

Die Berechnungsbasis der Verarbeitungskapazitäten beruht auf der Basiskonfiguration von Transactional Email. Die Messung legt eine Email-Größe von 200 Kilobytes zu Grunde und berücksichtigt Open- und Link-Tracking für einen Zeitraum von einer Stunde.

Eine vertraglich vereinbarte Verarbeitungskapazität auf stündlicher Basis setzt voraus, dass der Kunde alle bei Retarus eingehenden Versandaufträge, wie in dem Beispiel unten aufgeführt, über den Verlauf einer Stunde gleichmäßig verteilt Um den vertraglich vereinbarten Durchsatz darstellen zu können, überprüft Retarus die Verteilung in Fünf-Minuten-Intervallen.

Aufgrund möglicher Sende-Peaks kann die tatsächliche Verarbeitungskapazität das 1,25-Fache der vereinbarten Verarbeitungskapazität betragen. Abhängig von weiteren Funktionen bzw. größeren Emails kann sich die Bandbreite verringern. Abweichungen sind möglich. Für eine Erhöhung der Verarbeitungskapazität ist jeweils eine individuelle Anforderungsprüfung notwendig.

Rechenbeispiel – Verarbeitungskapazität

Im nachfolgenden Beispiel beträgt die vertraglich vereinbarte Verarbeitungskapazität 150.000 Emails/Stunde:

- (150.000 Emails/Stunde) / (12 x Intervall*/Stunde) = 12.500 Emails/Intervall*
- Die Kapazitätserweiterung für Sende-Peaks von 25 % kann den Durchsatz auf ein Maximum von bis zu 15.625 Emails/Intervall* erhöhen.

*Ein Intervall beträgt 5 Minuten.

IP-Whitelisting

Mit der Retarus IP-Whitelisting-Funktion kann der Kunde explizit definieren, welche Applikationen aus seinem Netzwerk via Transactional Email Nachrichten versenden dürfen.

Feedback Loops

Retarus steht mit verschiedenen ISPs (Internet-Service-Providern) über eine Beschwerde-Vereinbarung in Verbindung. Beschwerdeinformationen werden von teilnehmenden ISPs in Form von Feedback-Loops (ARF) an Retarus zurückgemeldet.

Feedback-Loops ist ein vom ISP zur Verfügung gestellter Mechanismus, um Versender darüber zu informieren sobald Nachrichten des Kunden als unerwünscht klassifiziert worden sind. Als in diesem Sinne unerwünscht gelten Emails, die Empfänger als Spam einstufen, z. B. durch einen Klick auf „Dies ist Spam“ im eigenen Postfach).

Beschwerden werden in einem automatisierten Verfahren rückgeführt, in dem die übermittelten Beschwerdeinformationen von Retarus ausgelesen und übermittelt werden – per Email an die zur Verfügung stehende Reply-To-Adresse oder via API-Callback an einen bereitstehenden Webservice des Kunden. Nach erfolgreicher Übertragung werden alle diesbezüglichen Informationen zur Beschwerde gelöscht und nicht archiviert.

Email-Abrechnung

Emails werden je Einheit abgerechnet, wobei eine abrechenbare Einheit 200 Kilobytes beträgt. Emails, die größer als 200 Kilobytes sind, werden entsprechend in mehrere Einheiten zum Zwecke der Abrechnung aufgeteilt.

Beispiel: Eine Email hat eine Größe von 2.403 Kilobytes (ca. 2,4 MB) – dies entspricht 13 Abrechnungseinheiten

Emails werden unabhängig davon in Rechnung gestellt (Identifier: Email-ID), ob die Übertragung erfolgreich war oder nicht (z. B. wenn Emails blockiert oder gebounced wurden).

Anbindung an Retarus

Die Anbindung der Systeme des Kunden an die Retarus-Infrastruktur erfolgt in der Regel über das Internetverschlüsselungsprotokoll Transport Layer Security (TLS), um eine gesicherte Übertragung der Daten via SMTP zu gewährleisten. Je nach Beauftragung ist eine Anbindung via opportunistic TLS oder enforced TLS möglich.

Email Security Services können optional über ein Virtual Private Network (VPN) angebunden werden. Voraussetzung für eine Verbindung via VPN ist die gleichzeitige Anbindung an die Retarus-Rechenzentren in München und Frankfurt/Main (RZ DE 1 und RZ DE 2).

Mitwirkungspflichten

Der Kunde ist sich dessen bewusst, dass die erfolgreiche Nutzung der Retarus-Dienste und die Qualität der Dienstleistungserbringung wesentlich von seiner Mitwirkung abhängt. Der Kunde wird daher das ihm nach Vertragsabschluss zugesandte Implementation-Sheet innerhalb von fünf (5) Werktagen ausgefüllt zurücksenden, insbesondere die unten genannten Mitwirkungspflichten einhalten und erklärt sich damit einverstanden, dass Retarus zum Schutz der stabilen Dienstleistungserbringung und der ISP-Reputation der Parteien dienliche technische Maßnahmen ergreifen darf. Hierbei ist es Retarus ausdrücklich erlaubt, spezifische Email-Aufträge zu verwerfen, das Volumen zu drosseln oder im Extremfall den Zugang zu sperren. Entstehen durch die Nichteinhaltung der Mitwirkungspflichten Aufwände und/oder Kosten, sind diese vom Kunden zu tragen.

Einwilligung

Der Kunde sichert zu, Emails nur an Adressaten zu versenden, die nach den jeweils geltenden gesetzlichen Rahmenbedingungen hierzu ihre ausdrückliche Einwilligung erteilt haben (Opt-In) oder für die ein sonstiger rechtlich anerkannter Erlaubnistatbestand gegeben ist.

Gestaltung der Email

Jede versendete Email muss ein den geltenden rechtlichen Anforderungen entsprechendes, leicht erkennbares Impressum, im Volltext einer jeden Email, enthalten.

Für den Versand von Emails mit Werbeinhalten gilt zudem:

- Der Auftraggeber einer Werbesendung muss klar erkennbar sein.
- In jeder Email ist der Empfänger gesondert auf die Möglichkeit hinzuweisen, die erteilte Einwilligung in die Zusendung von Emails jederzeit zu widerrufen. Der Widerruf / das Abbestellen von Emails (Opt-Out / Unsubscribe) muss dem Empfänger grundsätzlich ohne Weiteres, d. h. ohne die Eingabe von Zugangsdaten (z. B. Login und Passwort) möglich sein.
- In der Kopf- und Betreffzeile der Email darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

Technische Konfiguration

- Absenderadressen sind registrierungspflichtig und Bestandteil der Service-Administration. Die Absenderadresse muss in der Lage sein, Emails zu empfangen (valider DNS-MX-Record). Die Absenderdomain muss zudem über einen validen DNS-A-Record verfügen. Rollenbasierende Absenderadressen (z. B. postmaster@) sind nicht erlaubt.
- Der Kunde muss Email-Adressen unverzüglich von den entsprechenden Mailinglisten entfernen, wenn nach dem Beschicken dieser Adressen die Nichtexistenz des Postfachs erkannt wird, spätestens jedoch, wenn drei Hard-Bounces erfolgt sind. Insgesamt darf die Hard-Bounce-Rate pro ISP 1,0 % grundsätzlich nicht übersteigen. Rollenbasierende Empfängeradressen (z. B. postmaster@) werden automatisch verworfen.
- Der Kunde muss Email-Adressen von den entsprechenden Mailinglisten entfernen, wenn der Empfänger die Email als SPAM einstuft (complaint) oder die Einwilligung in den Versand von Emails widerruft.
- Für die in der SMTP-Kommunikation zwischen Email- Servern angegebene „MAIL FROM“-Adresse ist ein SPF-From Record einzutragen, der es SPF-Systemen auf Empfängerseite erlaubt, einen SPF-Test durchzuführen. Der SPF-Record muss mit „-all“ oder „-~all“ enden. Sollten die nötigen Einträge kundenseitig nicht innerhalb von zehn (10) Werktagen erfolgen, wird die erneute Überprüfung nach Aufwand in Rechnung gestellt.

- Das Verfahren DKIM (DomainKeys Identified Mail) ist seitens des Kunden zwingend einzusetzen, d. h. für jede bei Retarus für den Kunden registrierte Absenderdomain hat der Kunde einen entsprechenden DKIM-Schlüssel in seinem DNS zu hinterlegen. Sollten die nötigen Einträge kundenseitig nicht innerhalb von zehn (10) Werktagen erfolgen, wird die erneute Überprüfung nach Aufwand in Rechnung gestellt.
- Jede versendete Email muss einen „List-Unsubscribe"-Header oder einen „List-Help“-Header (siehe RFC 2369) enthalten. Der „List-Unsubscribe“-Header ist für listenbasierte Mailings erforderlich und mit „POST HTTPS“-Link inklusive „One-Click-Unsubscribe“-Funktionalität (RFC 8058) einzufügen. Der angegebene Link muss eine direkte One-Click-Abmeldung mindestens auf Listenebene bewirken. Der Versender darf dem Nutzer eine Bestätigungs-Email für die erfolgte Abmeldung übersenden. Bei nicht-listenbasierten Mailings muss alternativ zum „List-Unsubscribe“-Header der „List-Help“-Header gesetzt werden. Der „List-Help“-Header muss mindestens eine „mailto:“-Adresse oder einen HTTPS-Link enthalten, HTTP-Links sind nicht zulässig. Sowohl die Verwendung der „mailto:“-Adresse als auch des HTTPS-Links müssen dem Empfänger die Möglichkeit geben, Informationen zu erhalten, aus welchem Grund die Email an ihn versendet wurde und weshalb eine Abmeldung auf Listenebene nicht möglich ist.

- Die Nutzung des „list-unsubscribe-Post“-Header erfordert einen valide URL, die entsprechende POST-Request entgegennehmen und verarbeiten kann.
  Beispiel:

```
List-Unsubscribe:      <mailto:listrequest@example.com?subject=unsubscribe>,
                       <https://example.com/unsubscribe.html?opaque=123456789>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

- Ausnahmen von dieser Verpflichtung können geltend gemacht werden, wenn es aus Gründen der Ausgestaltung des Dienstes und der damit einhergehenden Zusendung automatisierter Emails nicht erforderlich oder möglich ist, eine Abmeldung im vorgenannten Sinne durchzuführen.
- Retarus ist CSA-zertifiziert (Certified Senders Alliance). Die hier beschriebenen Mitwirkungspflichten entsprechen den aktuellen CSA-Vorgaben. Die CSA kann ihre Anforderungen jederzeit anpassen. Daher verpflichtet sich der Kunde, etwaige Anpassungen mitzutragen. Hierüber werden die Kunden entsprechend von Retarus informiert.

Implementierung, Change-Management und Support

Die Implementierung beginnt nach Auftragserteilung und Zusendung des vollständig und korrekt ausgefüllten Setup-Sheets durch den Kunden.

Für Support- und Serviceanfragen sowie Change Requests muss der Kunde Retarus den Kreis autorisierter Personen mitteilen, die solche Anfragen offiziell stellen dürfen. Der technische Ansprechpartner des Kunden für die Implementierung des Services wird dabei grundsätzlich als erster autorisierter Ansprechpartner festgelegt. Dieser kann sodann als Kundenadministrator im Enterprise Administration Portal weitere Support-Kontakte eintragen und somit autorisieren. Kunden-Administratoren können diese Berechtigungen jederzeit ändern, erweitern oder löschen.

Im Kundenauftrag umgesetzte Änderungen am Service und Lösungen für Incidents (inkl. Workarounds) müssen durch den Kunden mindestens in Textform abgenommen werden. Erfolgt innerhalb von 10 Tagen keine Rückmeldung durch den Kunden, wird das jeweilige Kundenticket nach Ablauf dieser Frist automatisch geschlossen und die Änderung / Lösung gilt als abgenommen.