

Sicher und erfolgreich mit digitaler Identitätsprüfung



- 2 EINLEITUNG
- 3 BETRUGSPRÄVENTION
- 4 IDENTITÄTSPRÜFUNGEN
- 5 eIDV CHECKLISTE
- 6 WARUM MELISSA?

EINLEITUNG

Die Zahl der Betrugsfälle mit gefälschten Identitäten nimmt stetig zu. So wurden etwa laut Statista¹ im Jahr 2023 in Deutschland rund 32.600 Geldwäschedelikte polizeilich erfasst, was einen neuen Höchststand darstellt. Dabei gehen die Betrüger immer heimtückischer vor und nutzen moderne Technologien. Unternehmen, insbesondere aus dem Finanzdienstleistungssektor, sind daher gefordert, ihre Sicherheitskonzepte zu überdenken.

In diesem White Paper zeigen wir proaktive Maßnahmen zur Betrugsprävention auf, mit denen sich nicht nur finanzielle Verluste, sondern auch Imageschäden vermeiden lassen.

BETRUG IN NEUEN DIMENSIONEN

Eine neue, besonders heimtückische Form des Betrugs ist der synthetische Identitätsbetrug (Synthetic Identity Fraud, SIF). Dabei werden echte persönliche Daten wie gültige Sozialversicherungsnummern und Geburtsdaten mit gefälschten Daten wie falschen Adressen kombiniert und so neue Identitäten erschaffen. Diese können dann beispielsweise zur Eröffnung falscher Konten oder für illegale Einkäufe genutzt werden.

Weitere Beispiele sind die Fälschung von Ausweisdokumenten mittels KI-Algorithmen oder die Vortäuschung von Videokonferenzen mittels Deepfake-Technologien. Diese und viele weitere ausgeklügelte Betrugsmaschen sind mit veralteten Technologien nur sehr schwer oder gar nicht zu erkennen.

Die elf Datenqualitätskriterien sind die bekanntesten Kennzahlen, um Datenqualität zu messen (Quelle: Melissa Data GmbH)



DIE WICHTIGSTEN MASSNAHMEN ZUR BETRUGSPRÄVENTION

Unternehmen sind teilweise gesetzlich verpflichtet, die Identität von Personen oder Organisationen zu überprüfen. Unter Anti-Money Laundering (AML) werden Maßnahmen und Gesetze zusammengefasst, die Geldwäsche verhindern oder bekämpfen sollen. Dazu gehören die EU-Geldwäscherichtlinien, das Geldwäschegesetz (GwG) in Deutschland und der USA Patriot Act. Eine Identitätsprüfung umfasst folgende Maßnahmen:

- **Know Your Customer (KYC, dt. „Kenne deinen Kunden“)** bezeichnet die Identifizierung und Überprüfung von Neu- und Bestandskunden sowie Geschäftspartnern. Dazu gehört die Überprüfung von persönlichen Daten.
- **Know Your Business (KYB, dt. „Kenne dein Unternehmen“)** ist dem KYC-Prozess ähnlich, wobei der Schwerpunkt auf der Identifizierung und Überprüfung von Unternehmen und Lieferanten liegt. Eine KYB-Prüfung versetzt Finanzinstitute somit in die Lage, mögliche Risiken, die von neuen oder bestehenden Geschäftspartnern ausgehen, umfassend zu erkennen. Dies ist notwendig, da Betrug häufig über Briefkastenfirmen oder Organisationsstrukturen begangen wird, die in Wirklichkeit gar nicht existieren. Daher empfiehlt es sich, zusätzlich die Registernummer und den Unternehmensstatus zu überprüfen. Durch KYB-Checks kann das Risiko, Opfer solcher Betrugsmaschinen zu werden, erheblich reduziert werden.
- Die **Identifizierung politisch exponierter Personen, kurz PEP**, ist ein weiterer wichtiger Schritt zur Durchführung einer effektiven Sorgfaltsprüfung und Risikobewertung. Schließlich haben sie in der Regel eine prominente öffentliche Funktion inne oder sind mit einem entsprechenden Amt betraut. Da PEP einen leichteren Zugang zu öffentlichen Ressourcen und mehr Einfluss haben als normale Personen, gelten sie als besonders gefährdet, in Korruption, Bestechung oder Geldwäsche verwickelt zu werden. Unternehmen sollten daher laufend prüfen, ob Personen, mit denen sie Geschäftsbeziehungen unterhalten, auf einer sogenannten PEP-Liste stehen, die von Aufsichtsbehörden und internationalen Organisationen geführt wird und auf den Internetseiten der Regierungen zu finden ist. So hat beispielsweise die Europäische Kommission eine Liste mit wichtigen öffentlichen Ämtern auf nationaler Ebene, in internationalen Organisationen sowie in Organen und Einrichtungen der Europäischen Union² veröffentlicht. Personen, die diese Ämter bekleiden, gelten laut BaFin als PEP. Auch Presseveröffentlichungen sind eine verlässliche Quelle für Informationen über Personen in politischen Ämtern. Bei Geschäften mit PEP müssen Unternehmen erhöhte Sorgfalt walten lassen, um die Einhaltung der geldwäscherechtlichen Vorschriften zu gewährleisten.
- Bei **Sanktionslistenprüfungen** werden Namen und Adressen von Geschäftskontakten und Mitarbeitern mit den Einträgen in den einschlägigen Sanktionslisten³ abgeglichen. Sanktionen sind im Kontext der internationalen Beziehungen und des Völkerrechts Strafmaßnahmen oder Strafen, die von einer oder mehreren Regierungen oder internationalen Gremien gegen ein Land, eine Institution, eine Organisation oder eine Person verhängt werden. Unternehmen dürfen mit solchen Parteien keine Rechtsgeschäfte tätigen, ansonsten drohen empfindliche Bußgelder. Zudem schadet es der Reputation und führt zu einem Vertrauensverlust, wenn öffentlich bekannt wird, dass ein Unternehmen mit einer sanktionierten Institution oder Person Geschäfte getätigt hat.
- Im Rahmen eines **Adverse Media Screenings** wird geprüft, inwieweit Personen oder Unternehmen in der Medienberichterstattung negativ dargestellt werden. Dabei geht es insbesondere um die Frage, ob es Hinweise auf Geldwäsche, Finanzbetrug, Drogenhandel, finanzielle Bedrohungen oder organisierte Kriminalität, Terrorismus, Cyberkriminalität, Gewalt- oder Sexualdelikte gibt. Die damit verbundenen Herausforderungen sind aufgrund der Vielzahl der Quellen groß. Das Spektrum reicht von Zeitungen und Zeitschriften über Radio und Fernsehen bis hin zu Pressemitteilungen, Blogbeiträgen oder Inhalten auf Websites. Diese Medienvielfalt bzw. die zunehmende Informationsflut macht es praktisch unmöglich, die Nachrichtenlage manuell zu überwachen. Hinzu kommen mögliche Tippfehler bei der Recherche und die Gefahr, dass Suchmaschinen Einträge noch gar nicht indexiert haben und diese somit unberücksichtigt bleiben. Adverse Media Screenings müssen kontinuierlich durchgeführt werden. Denn wenn die Prüfung nur bei der Anbahnung einer neuen Geschäftsbeziehung erfolgt, entsteht lediglich eine Momentaufnahme. Es ist aber durchaus möglich, dass ein Kunde oder Lieferant zu diesem Zeitpunkt „sauber“ ist und erst später in Verruf gerät.

Ergänzend ist es sinnvoll, eine **Identitätsverifizierung** durchzuführen. Dabei werden die Gesichtsmarkale, die während des Onboarding-Prozesses mit einem Echtzeit-Selfie aufgenommen werden, mit den Merkmalen auf dem vom Interessenten vorgelegten Ausweisdokument abgeglichen (Biometrics). Beim Liveness Check schließlich hält der Nutzer sein Gesicht in die Kamera und bewegt seine Augen, um sicherzustellen, dass die gezeigte Person echt ist.

WELCHE UNTERNEHMEN MÜSSEN IDENTITÄTSPRÜFUNGEN DURCHFÜHREN?

Grundsätzlich hat jedes Unternehmen, unabhängig von der Branche, ein Interesse daran, Prozesse zur digitalen Identitätsprüfung einzuführen, um Compliance-Vorschriften einzuhalten, Betrugsfälle zu reduzieren und das Vertrauen der Kunden zu stärken. Je nach Branche gibt es aber noch weitere Argumente, die für eine Identitätsprüfung sprechen:

- Finanzdienstleister wie Banken, Versicherungen und andere Institute wollen das Onboarding von Kunden so einfach wie möglich gestalten, um die Zahl der Kontoeröffnungen zu erhöhen. Gleichzeitig unterliegen sie strengen Vorschriften zur sorgfältigen Überprüfung der Identität ihrer Kunden.
- Betreiber von digitalen Wettbüros, Online-Casinos oder Spieleplattformen haben ein Interesse daran, die Zahl der Registrierungen zu erhöhen. Gleichzeitig sind sie gefordert, das Alter ihrer Kunden zu überprüfen und sich vor Betrug zu schützen.
- Krankenhäuser und Arztpraxen müssen die Identität von Patienten überprüfen, um eine ordnungsgemäße medizinische Versorgung zu gewährleisten und Verwechslungen zu vermeiden.
- Mobilfunkanbieter sind nach dem Telekommunikationsgesetz (TKG) zur Identitätsprüfung bei der Registrierung von Prepaid-SIM-Karten verpflichtet.
- E-Commerce-Anbieter und Händler sind beim Verkauf von altersbeschränkten Produkten wie Alkohol, Tabak oder Filme mit Altersfreigaben verpflichtet, das Alter und in einigen Fällen die Identität des Kunden zu überprüfen, um sicherzustellen, dass das Produkt nicht an Minderjährige verkauft wird. Darüber hinaus schreibt das GwG vor, dass Händler, die Transaktionen über einem bestimmten Schwellenwert abwickeln, die Identität ihrer Kunden überprüfen müssen.
- Auch Immobilienmakler sind nach dem GwG verpflichtet, Identitätsprüfungen durchzuführen.

IDENTITÄTSPRÜFUNG BEIM ONBOARDING

Digitales Onboarding wird heute immer beliebter, sei es beim Bestellen im Shop, beim Abschluss einer Versicherung, bei der Eröffnung eines Kontos oder beim Beitritt zu einer Plattform. Dabei spielt die Identitätsprüfung in den genannten Branchen eine zentrale Rolle. Hierfür können verschiedene Methoden wie das Scannen von Dokumenten, die biometrische Authentifizierung und die Validierung von Ausweisdokumenten eingesetzt werden. Kunden, die an den Komfort von Apple oder Amazon gewöhnt sind, empfinden aber zusätzliche Sicherheitsabfragen oder das Einreichen von Dokumenten als lästig. Diese

Maßnahmen wirken antiquiert, kosten Zeit und sind mit Aufwand verbunden. Mit automatisierten Prozessen und entsprechenden Softwarelösungen lassen sich regulatorische Anforderungen dagegen effektiver umsetzen, wie das folgende Praxisbeispiel zeigt:

Ein Unternehmen bietet seinen Kunden die ortsunabhängige Anmietung von Fahrzeugen an. Damit sich Neukunden vollständig online registrieren können, hat es eine Lösung zur Validierung und Verifizierung internationaler Adressen eingeführt. Diese prüft, ob die von den Kunden eingegebenen Informationen plausibel und korrekt sind. Ist dies der Fall, folgt die Identitätsprüfung. Dabei werden die persönlichen Daten des Kunden – Name, Adresse und Geburtsdatum – geprüft, mit Referenzdaten abgeglichen und verifiziert. Auf diese Weise kann das Unternehmen die Kundenzufriedenheit deutlich steigern.

HOHE DATENQUALITÄT ALS BASIS FÜR BETRUGSPRÄVENTION

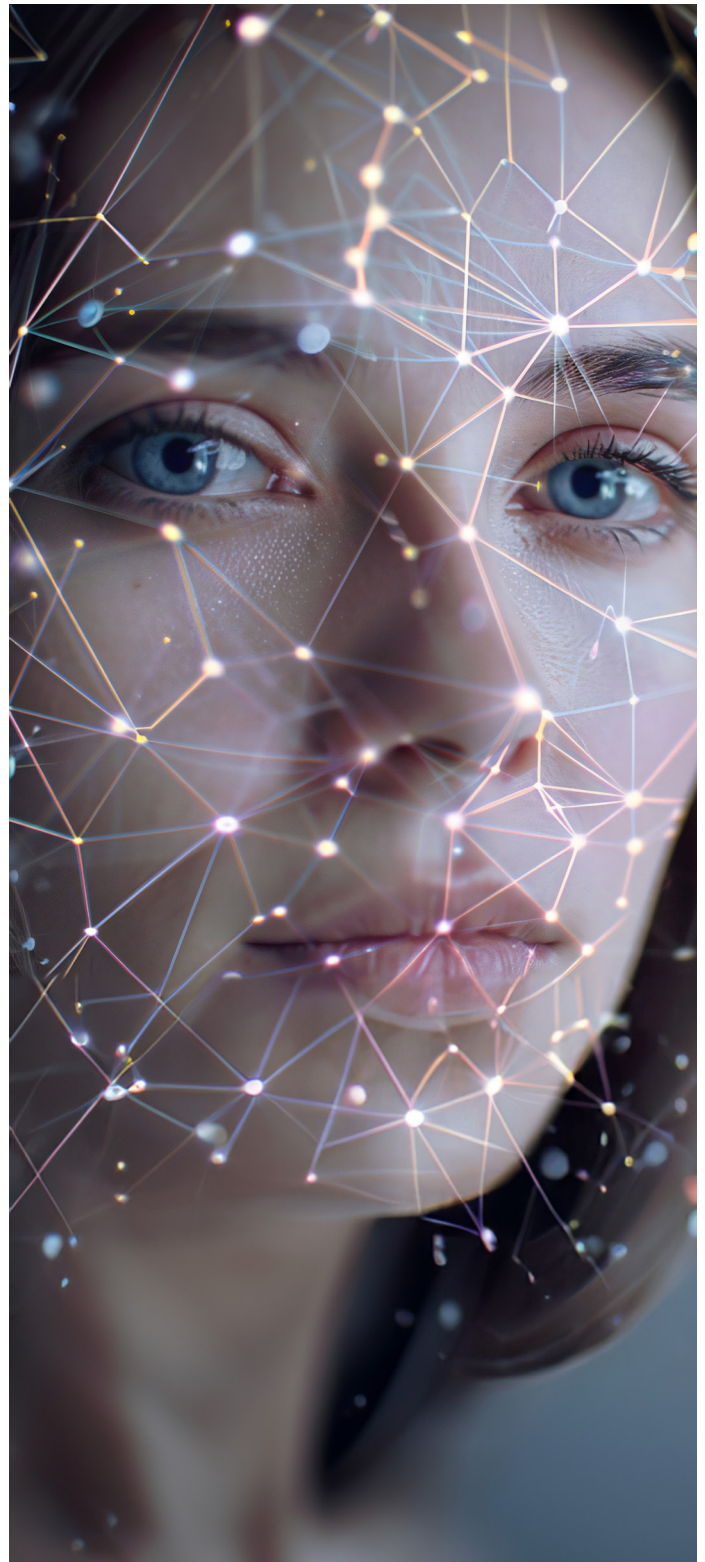
Damit Unternehmen die Identitäten ihrer Kunden zuverlässig überprüfen können, ist eine hohe Datenqualität unabdingbar. Sie beschreibt den Zustand der Daten anhand von Faktoren wie Korrektheit, Konsistenz, Aktualität, Einheitlichkeit und Genauigkeit. Je besser diese Kriterien erfüllt sind, desto höher ist die Datenqualität. Um diese zu gewährleisten, ist eine kontinuierliche Datenpflege notwendig. Erfolgt diese manuell, werden wertvolle Personalressourcen gebunden, die für wertschöpfende Tätigkeiten eingesetzt werden könnten. Daher empfiehlt sich der Einsatz bewährter Softwareprodukte, die folgende Bereiche abdecken:

- Adressvalidierung behebt Fehler in nationalen und internationalen Adressen,
- Adress-Autovervollständigung ergänzt bei der Eingabe und beschleunigt so die korrekte Datenerfassung,
- E-Mail-Validierung korrigiert Fehler in E-Mail-Adressen,
- Namensvalidierung ermöglicht die Eliminierung von Fehlern in Namen oder Geschlechtsangaben,
- Dublettenprüfung identifiziert redundante Datensätze, um eine korrekte Datenbasis zu gewährleisten.

WORAUF SOLLTEN UNTERNEHMEN BEI DER AUSWAHL EINES ANBIETERS VON LÖSUNGEN ZUR ELEKTRONISCHEN IDENTITÄTSPRÜFUNG ACHTEN?

Bei der Auswahl eines Anbieters von Technologien zur Betrugsprävention sollten Unternehmen eine Reihe von Kriterien berücksichtigen, um sicherzustellen, dass die gewählte Lösung ihren spezifischen Anforderungen entspricht. Im Folgenden sind einige wichtige Aspekte aufgeführt:

- **Angemessene Betrugserkennungsfunktionen:** Der Technologieanbieter sollte eine breite Palette an Betrugserkennungsfunktionen offerieren, um verschiedene Betrugsarten abzudecken, die für die jeweilige Branche relevant sind. Dazu gehören die Adressvalidierung, das Screening nach politisch exponierten Personen (PEP), der Abgleich mit Sanktionslisten und anderen nationalen und internationalen Beobachtungslisten sowie das Screening nach negativen Meldungen.
- **Internationalität:** Das Internet kennt bekanntlich keine Grenzen, so dass entsprechende Betrugsdelikte weltweit geplant und begangen werden. Daher sollte die Lösung zur elektronischen Identitätsprüfung möglichst viele Länder abdecken.
- **Flexibilität:** Die Lösung zur elektronischen Identitätsprüfung sollte sich an die konkreten Anforderungen und das Risikoprofil des Unternehmens anpassen lassen. Individuelle Konfigurationen sowie Regelwerke und Schwellwerte, die auf spezifische Geschäftsprozesse zugeschnitten werden können, sind dabei unerlässlich. Darüber hinaus sollte die Lösung skalierbar sein, um sich an unterschiedliche Transaktionsvolumina anzupassen.
- **Warnmeldungen in Echtzeit:** Die in der Lösung zur elektronischen Identitätsprüfung integrierten Überwachungs- und Warnfunktionen sollten Betrugsfälle sofort melden, sodass Unternehmen umgehend darauf reagieren können.
- **Hohe Integrationsfähigkeit:** Eine nahtlose Integration in bestehende Systeme wie E-Commerce-Plattformen, Payment Gateways, Kundendatenbanken oder Risikomanagementsysteme ermöglicht einen effizienten Datenaustausch und optimierte Arbeitsabläufe.
- **Datenschutz und Datensicherheit:** Die Identitätsprüfung erfordert den Umgang mit sensiblen Kundendaten und Transaktionsinformationen. Daher sollte der Anbieter einer solchen Lösung technische und organisatorische Maßnahmen nachweisen, die den Datenschutz und die Datensicherheit gewährleisten.



WIE KANN MELISSA BEI DER IDENTITÄTSPRÜFUNG HELFEN?

Betrugsprävention ist heute eine der größten Herausforderungen für Unternehmen. Mit uns als Partner können Sie Risiken reduzieren, Ihre Compliance sicherstellen und auf ein besseres Kundenerlebnis hinwirken, was die Zufriedenheit steigert. Unsere elektronische Identitätsprüfung (eIDV) ist ein internationaler Echtzeit-Service, der Namen, Telefonnummern, Anschriften und E-Mail-Adressen prüft und standardisiert sowie die Identität eines Kunden bestätigt. Unser Web Service für weltweite Datenvalidierung stellt sicher, dass nur Kontaktdaten mit gültigen Kundeninformationen einer digitalen Identitätsprüfung unterzogen werden. Denn Kontaktdaten müssen vorab immer plausibilisiert werden, um die Qualität der anschließenden Datenverifizierung zu optimieren. Dazu gehören insbesondere Name, Anschrift, E-Mail-Adresse und Telefonnummer. Ein Abgleich mit nicht validierten bzw. standardisierten Daten kann dazu führen, dass ein Match mit offiziellen Referenzdatenquellen nicht erfolgreich durchgeführt werden kann, was wiederum die Anzahl der False Positives erhöht. Das kann unter Umständen die Ergebnisse sogar noch verschlechtern. Ein Technologieanbieter wie Melissa, der auf Datenqualität für internationale Kontaktdaten spezialisiert ist, kann bessere Ergebnisse liefern, da die Personendaten zunächst validiert, formatiert, standardisiert und dann zuverlässig mit offiziellen eIDV-Quellen verifiziert werden – und das international. So lässt sich sicherstellen, dass der komplette Datensatz vertrauenswürdig ist.

Folgende Möglichkeiten stehen Ihnen konkret zur Verfügung:

- Überprüfung und Vervollständigung von Kundendaten für mehr als 240 Länder und Territorien, einschließlich der Korrektur und Standardisierung internationaler Adressen im Länderformat. Über sechs Millionen Nachnamen und vier Millionen Vornamen können erkannt werden.
- E-Mail-Adressen können bis auf Postfachebene verifiziert werden. Darüber hinaus stellen wir sicher, dass Telefonnummern aktiv und anrufbar sind.
- Im Rahmen eines Proof of Address verknüpfen wir den Namen einer Person mit einer bestimmten Adresse, um den Adressnachweis in Echtzeit zu führen. Unter Nutzung von mehr als zwei Milliarden Datensätzen gewährleisten wir, dass die Person tatsächlich an der angegebenen Adresse wohnt.
- Unsere Lösung kann auch eine vollständige elektronische Identitätsprüfung durchführen, indem sie die Sozialversicherungsnummer, die nationale ID und das Geburtsdatum verifiziert.
- Wir prüfen, ob Personen oder Unternehmen inklusive ihrer Mitarbeiter auf einer Sanktions- bzw. PEP-Liste stehen oder in den Medien negativ aufgefallen sind (Adverse Media Screening). Dabei decken wir weltweit mehr als 200 Länder und Territorien ab. Alle entsprechenden Referenzdaten werden täglich in unseren Echtzeitumgebungen aktualisiert. Eine vollständige Aufstellung unserer Screening-Listen finden Sie [hier](#).

Selbstverständlich sind sowohl unsere elektronische Identitätsprüfung als auch alle anderen Lösungen datenschutzkonform. Grundsätzlich nehmen wir Datenschutz, Datensicherheit und die Einhaltung gesetzlicher Vorschriften und Verordnungen wie der **DSGVO** sehr ernst und führen laufend unabhängige Sicherheitsaudits durch. Zudem stehen unsere Server in Europa, insbesondere in Deutschland. Die Anfragen unserer europäischen Kunden laufen über diese Server und werden auch hier in Europa geroutet. Darüber hinaus haben wir professionelle Unterstützung durch externe Datenschutzbeauftragte und arbeiten in diesem Bereich mit der renommierten Kanzlei Kinast zusammen, die sich auf den nationalen Datenschutz spezialisiert hat und zahlreiche deutsche Unternehmen betreut. Darüber hinaus sind wir nach **SOC 2 Typ 1 und Typ 2 zertifiziert**. Damit können wir nachweisen, dass wir eine Bewertung unserer Kontrollaktivitäten durchgeführt haben, die sich auf die anwendbaren Trust Services Prinzipien und Kriterien bezieht.

Übrigens: Gartner hat unsere Lösungen bereits dreimal im **Magic Quadrant for Data Quality Solutions** gelistet. Darüber hinaus sind wir stolz darauf, von **G2-Anwendern als Top Leader 2024 für Datenqualität** ausgezeichnet worden zu sein. Unser Engagement für die Bereitstellung der besten Datenqualitätssoftware spiegelt sich in diesen Bewertungen wider:

- 97% einfache Geschäftsabwicklung
- 92% erfüllt Anforderungen
- 96 % einfache Bedienung
- 96 % einfache Einrichtung
- 90 % Benutzerfreundlichkeit

FAZIT:

Das Thema Online-Betrug gewinnt leider immer mehr an Bedeutung, weshalb Unternehmen mehr denn je gefordert sind, zuverlässige Präventionsmaßnahmen zu implementieren. Mit unseren skalierbaren Lösungen können Sie Ihr Unternehmen nachhaltig vor Betrug und den damit verbundenen Risiken schützen. Gleichzeitig können Sie Compliance-Anforderungen erfüllen und im Rahmen des digitalen Onboardings eine einfache und schnelle Registrierungsmöglichkeit schaffen, die das Kundenerlebnis optimiert.



www.melissa.de

Über Melissa

Melissa ist ein führender Anbieter von Datenqualitäts-, Identitätsprüfungs- und Adressmanagementlösungen. Melissa unterstützt Unternehmen bei der Kundengewinnung und -bindung, bei der Validierung und Korrektur von Kontaktdaten, bei der Optimierung des Marketing-ROIs sowie beim Risikomanagement. Seit 1985 ist Melissa für Unternehmen wie die Mercury Versicherung, Xerox, Disney, AAA und Nestlé ein zuverlässiger Partner bei der Verbesserung der Kundenkommunikation.

Deutschland

Cäcilienstr. 42-44
50667 Köln

+49 (0) 221 97 58 92 40

U.S.

1 800 MELISSA (635 4772)

CANADA

1 800 635 4772

INDIA

+91 (0)80 4854 0142

UK

+44 (0)20 7718 0070

AUSTRALIA

+61 02 8091 6000

SINGAPORE

+65 8 2997442