We record & analyze communications

Data Privacy Policy

Inhaltsverzeichnis

Geltungsbereich dieses Dokuments: ASC Technologies AG, Seibelstraße 2-4, 63768 Hoesbach, Deutschland, sowie die mit ihr gemäß § 15 AktG verbundenen Unternehmen die vom aktuellen Geltungsbereich der entsprechenden ISO-Zertifizierung erfasst sind.

Data Privacy Policy DE

1. Vision

Als weltweit führender Anbieter von Omnichannel-Aufzeichnung, Qualitätsmanagement und KI-basierter Analytik bietet die ASC Technologies AG („ASC“, „wir“) modernste Lösungen für die Steuerung digitaler Kommunikation und betrachtet den Schutz personenbezogener Daten und die Informationssicherheit als grundlegende Bestandteile ihrer Unternehmensstrategie und als freiwillige Verpflichtung zur Umsetzung für die gesamte ASC-Gruppe („ASC“). Die spezielle Datenschutzrichtlinie von ASC stellt daher höchste Anforderungen an die vollständige Einhaltung der DSGVO, des BDSG, des HIPAA und anderer relevanter Gesetze und behördlicher Anforderungen, um Technologien wie Cloud Computing und darauf basierende Dienste selbst nutzen, vor allem aber auch Kunden als innovative Dienste anbieten zu können. ASC ist bestrebt, seine Maßnahmen stets nach dem aktuellen Stand der Technik umzusetzen, um ein Höchstmaß an Sicherheit zu gewährleisten.

2. Mission

Diese Richtlinie legt den Rahmen für den Umgang mit personenbezogenen Daten bei ASC und die Umsetzung eines Datenschutzmanagementsystems („DMS“) fest, das bei allen Geschäftsaktivitäten von ASC einzuhalten und zu befolgen ist. ASC erfüllt die Anforderungen von Art. 32 DSGVO und stützt sich auf etablierte Sicherheitsstandards, um ein angemessenes Schutzniveau zu gewährleisten. Die Informationstechnologie ist nach DIN EN ISO/IEC 27001 und SOC 2 Typ II zertifiziert und basiert auf dem IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik. Darüber hinaus hat ASC zusätzliche Sicherheits- und Datenschutzmaßnahmen implementiert, um die Einhaltung der HIPAA-Anforderungen zu gewährleisten.

3. Grundsätze

Datenschutz-Managementsystem (DMS)

Zu diesem Zweck hat ASC ein umfassend dokumentiertes DMS mit detaillierten Verfahrensanweisungen implementiert. Diese dienen als Leitlinien für die Umsetzung datenschutzrelevanter Prozesse und ermöglichen eine transparente Nachverfolgbarkeit der Maßnahmen. ASC hat einen betrieblichen Datenschutzbeauftragten (DSB), einen Datenschutzkoordinator (DSK) und einen Informationssicherheitsbeauftragten (ISB) ernannt, um dieses DMS sicherzustellen. Diese Funktionen sind für die Überwachung, Kontrolle und Weiterentwicklung der Datenschutz- und Informationssicherheitsmaßnahmen verantwortlich und gewährleisten die Einhaltung der DSGVO, HIPAA und anderer relevanter gesetzlicher und regulatorischer Anforderungen.

Datenschutz-Folgenabschätzungen (DSFA)

ASC führt DSFA für Verarbeitungsaktivitäten durch, die wahrscheinlich hohe Risiken für die Rechte und Freiheiten von Personen mit sich bringen. Dazu gehören ausdrücklich alle Verarbeitungsaktivitäten, die elektronische Patienteninformationen (ePHI) betreffen. Die Ergebnisse der DSFA werden dokumentiert und als Grundlage für Entscheidungsprozesse im Zusammenhang mit dem Datenschutz herangezogen.

Technisch-organisatorische Maßnahmen (TOM)

In Übereinstimmung mit Artikel 35 DSGVO hat ASC technische und organisatorische Maßnahmen (TOM) definiert, die von der IT-Abteilung, ISB, DSB und DSK umgesetzt, gepflegt und kontinuierlich weiterentwickelt werden. Dazu gehören beispielsweise

- die Implementierung sicherer IT-Systeme
- Sicherung von Netzwerken und Verschlüsselung sensibler Daten
- regelmäßige Überprüfung und Aktualisierung der eingesetzten Sicherheitsmaßnahmen.

Die TOM basieren auf den anerkannten Standards der DIN EN ISO/IEC 27001 und dem deutschen BSI-IT-Grundschutz-Kompendium. Darüber hinaus sind diese TOM speziell auf die Sicherheitsvorschriften der HIPAA ausgerichtet, insbesondere hinsichtlich des Schutzes von ePHI, einschließlich Zugriffskontrollen, Verfügbarkeitskontrollen, Integritätskontrollen und Übertragungssicherheit. Diese Maßnahmen gewährleisten, dass personenbezogene Daten und ePHI wirksam vor unbefugtem Zugriff, Verlust oder Manipulation geschützt sind.

Automatisierte und nicht automatisierte Verarbeitung

Die Anforderungen dieser Richtlinie und des DMS gelten für alle Prozesse, in denen ASC personenbezogene Daten oder ePHI von Personen – insbesondere Mitarbeitern, Kunden, Lieferanten oder anderen Vertrags- und Geschäftspartnern – vollständig oder teilweise automatisiert (z. B. mittels elektronischer Datenverarbeitung) in Übereinstimmung mit der DSGVO verarbeitet.

Diese Anforderungen gelten auch für die nicht automatisierte Verarbeitung, wenn personenbezogene Daten oder ePHI in einer strukturierten Sammlung gespeichert sind oder gespeichert werden sollen, die nach bestimmten Kriterien zugänglich ist (z. B. in papierbasierten Personal-, Kunden- oder Projektakten).

Interne Audits und Kontrollen

Der Datenschutzbeauftragte und der Datenschutzkoordinator von ASC führen regelmäßig interne Audits und Kontrollen durch, insbesondere der TOMs. Diese internen Audits dienen der systematischen Überprüfung der Umsetzung und der Wirksamkeit der festgelegten Datenschutz-, HIPAA-Compliance-, ePHI-Schutz- und Sicherheitsmaßnahmen. Im Rahmen der Audits werden potenzielle Schwachstellen identifiziert und geeignete Maßnahmen zur Optimierung eingeführt. Die Ergebnisse der Audits werden dokumentiert und dienen als Grundlage für weitere Verbesserungen.

Schulung und Sensibilisierung

Um die Einhaltung der Datenschutz- und Sicherheitsanforderungen zu gewährleisten, werden die Mitarbeiter von ASC von Anfang an regelmäßig geschult und sensibilisiert. Die Schulungsmaßnahmen vermitteln praktisches Wissen über Datenschutzanforderungen, die Definition von ePHI, die richtigen Verfahren für den Umgang mit und den Schutz von ePHI sowie Sicherheitsrichtlinien und konkretes Verhalten in der täglichen Arbeit. Insbesondere werden die Grundprinzipien gemäß Art. 5 DSGVO vermittelt, wie z. B. das Prinzip der Datenminimierung oder das Prinzip der doppelten Kontrolle. Kontinuierliche Sensibilisierungsmaßnahmen fördern das Bewusstsein für Datenschutz und Datensicherheit im gesamten Unternehmen.

Verpflichtung der Mitarbeiter

Alle Mitarbeiter von ASC sind verpflichtet, die Datenschutzbestimmungen einzuhalten und Verschwiegenheit zu wahren. Diese Verpflichtung wird schriftlich festgehalten und umfasst den sorgfältigen und verantwortungsvollen Umgang mit personenbezogenen Daten, den Schutz von ePHI und die Einhaltung der HIPAA-Anforderungen. Die Mitarbeiter werden außerdem ausdrücklich angewiesen, Verstöße oder vermutete Verstöße im Zusammenhang mit Datenschutz und Datensicherheit unverzüglich zu melden.

Weitergabe von Daten an Dritte

ASC gibt personenbezogene Daten ausschließlich an seinen Drittanbieter Microsoft Azure weiter. ASC hat vertragliche Vereinbarungen mit Microsoft Azure getroffen, um sicherzustellen, dass alle Datenverarbeitungsaktivitäten in Übereinstimmung mit der DSGVO, HIPAA und anderen relevanten Vorschriften durchgeführt werden. Diese vertraglichen Vereinbarungen, einschließlich gegebenenfalls Business Associate Agreements (BAA), regeln ausdrücklich die HIPAA-Konformität für alle ePHI, die auf Microsoft Azure verarbeitet oder gespeichert werden. Externe Prüfer führen regelmäßige Audits und Bewertungen durch, um die fortlaufende Einhaltung der Vorschriften zu überwachen und potenzielle Risiken im Zusammenhang mit der Weitergabe von Daten an Dritte zu beseitigen.

Vorfallmanagement

ASC verfügt über eine nach ISO 27001 zertifizierte Richtlinie zum Vorfallmanagement, die darauf ausgelegt ist, Datenschutzvorfälle umgehend zu bearbeiten und zu mindern. Im Falle einer potenziellen Datenverletzung oder eines Sicherheitsvorfalls verpflichtet sich ASC, die betroffenen Kunden innerhalb von 72 Stunden oder gemäß anderweitigen vertraglichen Vereinbarungen zu informieren. Bei Vorfällen im Zusammenhang mit ePHI hält sich ASC an die Meldepflichten der HIPAA und benachrichtigt die betroffenen Personen, den Minister für Gesundheit und Soziales und in einigen Fällen auch die Medien, wie gesetzlich vorgeschrieben. Diese Richtlinie enthält detaillierte Verfahren für die Erkennung, Meldung und Behebung von Vorfällen, um sicherzustellen, dass Störungen der Datensicherheit effizient und transparent behandelt werden. Die Prozesse zum Vorfallmanagement werden kontinuierlich überwacht und regelmäßig überprüft, um die Wirksamkeit der Richtlinie zu verbessern und das Engagement von ASC für Datenschutz und Informationssicherheit aufrechtzuerhalten.

Aufbewahrung und Löschung von Daten

ASC speichert personenbezogene Daten, einschließlich ePHI, nur so lange, wie es zur Erfüllung der Zwecke, für die sie erhoben wurden, erforderlich ist oder wie es die geltenden Gesetze und Vorschriften vorschreiben, einschließlich der Aufbewahrungsfristen für ePHI gemäß HIPAA. Nach Ablauf der Aufbewahrungsfrist stellt ASC sicher, dass personenbezogene Daten sicher gelöscht werden. Detaillierte Verfahren zur Aufbewahrung und Löschung von Daten werden dokumentiert und regelmäßig überprüft, um die Einhaltung der Datenschutzanforderungen sicherzustellen.

4. Kontinuierliche Verbesserung

ASC ist bestrebt, die Wirksamkeit und Eignung seines DMS kontinuierlich zu verbessern, indem es dessen Wirksamkeit bewertet, Abweichungen behebt und gegebenenfalls Korrekturmaßnahmen ergreift. Das Feedback von Mitarbeitern und Kunden wird als wichtiger Motor für Wachstum und Leistungsoptimierung geschätzt.

5. Verantwortlichkeit und regelmäßige Überprüfung

Der Vorstand von ASC übernimmt die Verantwortung für die Wirksamkeit des Multi-Managementsystems und stellt sicher, dass diese Datenschutzrichtlinie im gesamten Unternehmen kommuniziert, verstanden und angewendet wird. Alle Mitarbeiter sind dafür verantwortlich, die festgelegten Prozesse einzuhalten und so zur kontinuierlichen Verbesserung beizutragen. Der Vorstand überprüft regelmäßig das MMS und aktualisiert diese Richtlinie, um ihre fortdauernde Angemessenheit und Wirksamkeit sicherzustellen.

6. Kommunikation

Diese Datenschutzerklärung ist für interne und externe Interessenten („Stakeholder“) öffentlich zugänglich. Anfragen können an folgende Adresse gerichtet werden: data.protection@asc.de.