COMPLIANCE-CHECKLISTE FÜR GESUNDHEITSDATEN

Als die Datenschutz-Grundverordnung (DSGVO) und der Data Protection Act (DPA 2018) im Jahr 2018 in Kraft traten, versuchten Unternehmen, die mit Bürgern des Vereinigten Königreichs und der EU Geschäfte machen, schnellstmöglich nötige Änderungen beim Datenschutz umzusetzen und die neuen Anforderungen zu erfüllen. Seitdem wurden mehrere zusätzliche Datenschutzgesetze vorgeschlagen und/oder umgesetzt: der Daten-Governance-Rechtsakt, das Datengesetz, die Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) und zuletzt die Verordnung über den Europäischen Gesundheitsdatenraum (EHDS).

Wie können Sie sich also in dieser sich schnell verändernden Landschaft aus Vorschriften und Compliance-Initiativen zurechtfinden? Unser Tipp: Indem Sie bekannte Best Practices nutzen und Technologien einsetzen, die sicherstellen, dass für Gesundheitsdaten relevante Prozesse den Vorschriften entsprechen und die Datensicherheit gewahrt bleibt – jetzt und in Zukunft.*

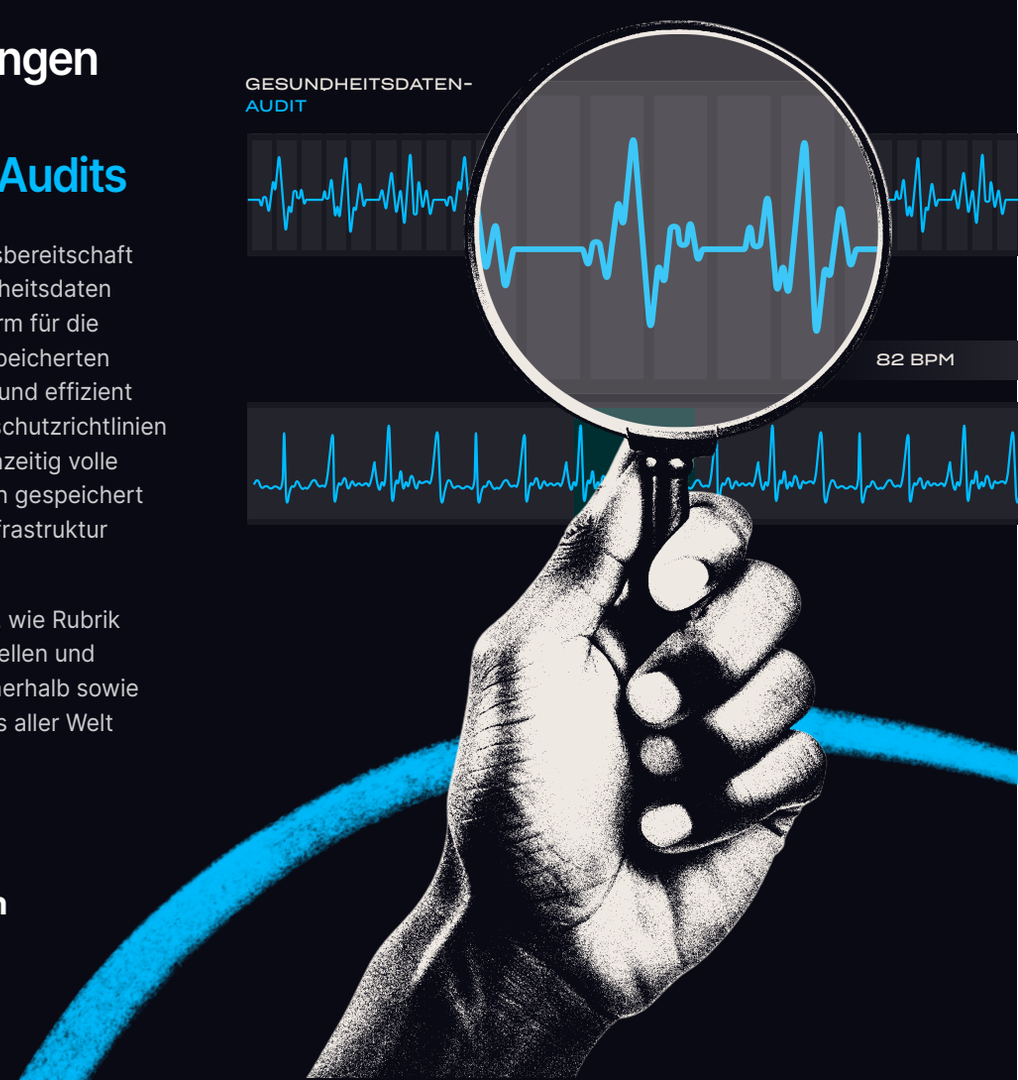
* Bitte beachten Sie, dass diese Seiten keine Rechtsberatung darstellen. Wir empfehlen, ein Gespräch mit einem auf die Compliance mit Datenschutzbestimmungen spezialisierten Anwalt zu vereinbaren, der aktuelle und kommende Datenschutzgesetze auf Ihre spezifischen Umstände anwenden kann.

Erfüllen Sie Compliance-Anforderungen für Gesundheitsdaten und sparen Sie Zeit bei Audits

Mit Rubrik können Sie Ihre Datensicherheitsbereitschaft verbessern und so Vorschriften für Gesundheitsdaten einhalten. Rubrik stellt eine zentrale Plattform für die Verwaltung aller lokal und in der Cloud gespeicherten Daten bereit, mit der Sie Vorgaben einfach und effizient umsetzen können. Benutzer können Datenschutzrichtlinien und deren Ablauf automatisieren und gleichzeitig volle Transparenz darüber erhalten, wo die Daten gespeichert sind und wie Richtlinien in der gesamten Infrastruktur eingehalten werden.

Kontaktieren Sie uns gern und erfahren Sie, wie Rubrik Organisationen bei der Einhaltung von aktuellen und zukünftigen Datenschutzbestimmungen innerhalb sowie außerhalb der EU unterstützt, um Daten aus aller Welt zu schützen.

Hier scannen, um mehr zu erfahren



GESUNDHEITSDATEN: IN 7 SCHRITTEN ZUR COMPLIANCE

rubrik

1

Definieren Sie Rollen und Zuständigkeiten

Legen Sie klar definierte Rollen und Zuständigkeiten fest, aus denen hervorgeht, wer jeweils für die einzelnen Schritte auf dem Weg zur Compliance verantwortlich ist. So könnte es beispielsweise in den Aufgabenbereich eines bestimmten Teams fallen, zu ermitteln, wie sensible Gesundheitsdaten derzeit erhoben und verwendet werden, wie aktuelle Datenrichtlinien und -kontrollen die Verwendung und Weitergabe personenbezogener Daten ermöglichen und wie Patienten derzeit Zugriff auf ihren Gesundheitsdaten anfordern und deren Löschung beantragen können.

2

Führen Sie eine Lückenanalyse durch

Überprüfen Sie die aktuellen Datenschutzrichtlinien und deren Umsetzung. Dabei sollten Sie nicht nur untersuchen, zu welchen Zwecken Sie Gesundheitsdaten verarbeiten und um welche Daten es sich dabei genau handelt, sondern auch wer innerhalb Ihrer Organisation auf diese Daten Zugriff hat und wie bzw. welche Dritte (z. B. Epic, Cerner, McKesson, BigHealth) Zugang erhalten. Außerdem empfiehlt es sich festzustellen, welche Maßnahmen Sie zum Schutz von Gesundheitsdaten bereits ergreifen und wie lange Sie Daten speichern wollen, bevor diese gegebenenfalls automatisch gelöscht werden. Vergleichen Sie die Ergebnisse Ihrer Analyse mit den Compliance-Anforderungen aktueller und zukünftiger Datenschutzvorschriften. So können Sie ermitteln, wo noch Handlungsbedarf besteht.

3

Erstellen Sie einen Aktionsplan

Stellen Sie einen Zeitplan für Prioritäten, Schritte und Maßnahmen auf, die notwendig sind, um die Einhaltung aktueller und zukünftiger Vorschriften zum Schutz von Gesundheitsdaten zu erreichen und aufrechtzuerhalten. Berücksichtigen Sie dabei relevante Gesetze, Datensicherheit, Rechenschaftspflicht, Governance und Datenschutzrechte.

4

Holen Sie sich Rückendeckung

Sensibilisieren Sie den Vorstand, um sicherzustellen, dass die Führungsetage Ihres Unternehmens die für die Einhaltung von Datengesetzen erforderlichen Änderungen akzeptiert und unterstützt. Es ist äußerst wichtig, dass Organisationen im Gesundheitswesen alle notwendigen Schritte unternehmen, um Gesundheitsdaten, geistiges Eigentum und andere geschäftskritische Daten ausreichend zu sichern. Nur so können erhebliche finanzielle Strafen vermieden werden, ganz zu schweigen von Rufschäden – oder dem Verlust von Menschenleben.

5

Sensibilisieren Sie die Belegschaft

Machen Sie Mitarbeiter – Benutzer, IT-Fachleute, Management usw. – auf die Änderungen, die sich aus geltenden Datenschutzvorschriften ergeben, aufmerksam und weisen Sie sie auf ihre Verantwortung im Hinblick auf diese Vorschriften hin. Mitarbeiterschulungen zu allen Aspekten der Datenschutzgrundsätze und der internen Richtlinien für die Datenverwaltung sind unerlässlich, damit im Gesundheitswesen tätige Organisationen Datenschutzverordnungen einhalten und gleichzeitig die ihnen anvertrauten, sensiblen Daten schützen.

6

Reformieren Sie Informations-Governance-Frameworks

Stellen Sie sicher, dass Ihre Informations-Governance (IG)-Frameworks den Anforderungen entsprechen. Überarbeiten Sie IG-Richtlinien, wie z. B. Richtlinien zur Aufbewahrung, zum Zugriff und zur Löschung von Daten, zur Datenverwaltung, zu Klassifizierungs- und Speicherverfahren, zur Notfallwiederherstellung und zu Sicherheitsprotokollen für digitale und papierbasierte sensible Datensätze. Setzen Sie zudem auf proaktive Überwachung zur Ermittlung potenzieller Schwachstellen, Datenschutzverletzungen, überprivilegierten Zugriffs und unbefugter Zugriffsversuche und -verfahren. So bringen Sie alles mit aktuellen (und zukünftigen) Anforderungen in Einklang.

7

Setzen Sie auf regelmäßige Audits

Durch das Aufstellen eines regelmäßigen Audit-Plans können Sie sicherstellen, dass Sie die Vorschriften einhalten und gleichzeitig die Ihnen von Privatpersonen anvertrauten sensiblen Daten schützen. Um regelmäßige Audits zu ermöglichen und die Compliance einfach und effizient zu gestalten, können Sie eine einzelne Plattform bereitstellen, die Datenmanagement für lokale und in der Cloud gespeicherte Daten erlaubt. Benutzer können Datenschutzrichtlinien und deren Ablauf automatisieren und gleichzeitig volle Transparenz darüber erhalten, wo sich die Daten befinden und wie Richtlinien in der gesamten Infrastruktur eingehalten werden.