WHITEPAPER

Zertifizierung des Datenschutzes gemäß Datenschutzstandard DGI-DSM (DGI®) in der Praxis

AOK PLUS

DGI® Deutsche Gesellschaft für Informationssicherheit AG

Unsere Expertise, Ihre Sicherheit!

INHALT

EINLEITUNG

Die Entwicklung der Informationstechnologie, mit weltweiter Vernetzung und Datenübermittlung sowie immer neuen Formen der elektronischen Kommunikation, führt für die Personen zunehmend zum Verlust der Kontrolle über die eigenen personenbezogenen Daten.

Die vermehrte Digitalisierung der Datenflüsse sowie die aktuelle technische Entwicklung führen zudem auf allen Seiten zu einer starken Verunsicherung bezüglich der rechtskonformen Ausgestaltung angemessener technischer und organisatorischer Maßnahmen zum Datenschutz.

Die Rechtsvorgaben wie die EU-Datenschutz-Grundverordnung, das Bundesdatenschutzgesetz oder die Sozialgesetzbücher, mit den teils uneindeutigen Regelungen, stellen Unternehmen vor große Herausforderungen bei der Bestimmung und Sicherstellung der Rechtmäßigkeit für eine rechtskonforme Verarbeitung personenbezogener Daten.

Insbesondere die Wahrung der Rechte der betroffenen Personen fordert den verantwortungsvollen wie zweckgebundenen Umgang mit personenbezogenen Daten sowie die frühzeitige Identifikation von Risiken, um diesen, proaktiv wie reaktiv, zeitgerecht und angemessen zu begegnen.

Den möglichen rechtlichen und ökonomischen Auswirkungen, wie der Anwendung von Strafvorschriften oder dem Verlust des Images, bei Datenpannen entgegenzuwirken sollte eine ausreichende Motivation für die Unternehmen darstellen.

Durch eine unabhängige und transparente Zertifizierung des Datenschutzes kann, insbesondere den eigenen Stakeholdern wie auch den Aufsichts- und Prüfinstanzen gegenüber, die Einhaltung der datenschutzrechtlichen Vorgaben sowie die Umsetzung der geforderten technischen und organisatorischen Maßnahmen bei der Verarbeitung von personenbezogenen Daten nachgewiesen werden.

Der Erwerb eines Datenschutzzertifikats und die zusätzliche Außendarstellung durch das Datenschutzsiegel können dafür verwendet werden, gegenüber den Kunden sowie den eigenen Beschäftigten, den Lieferanten und den Geschäftspartnern das erfolgreich umgesetzte Datenschutzniveau zu vermitteln und den Wettbewerbsvorteil im eigenen Marktumfeld darzustellen.

VORTEILE

Die Potentiale, die sich aus einer Zertifizierung des eigenen Datenschutzes ergeben, lassen sich besser erkennen, sofern die Motivation für eine Zertifizierung sowie die beabsichtigte Wirkung der Zertifizierung hinterfragt werden.

So sollten Fragen, ob die Zertifizierung eines Standortes, eines Geschäftsprozesses oder einer Dienstleistung beabsichtigt ist, beantwortet werden können. Zudem sollten sich Antworten auf die Fragen nach den Schwerpunkten der Auditierung, nach dem Fachwissen, der Qualifikation und den Erfahrungen der Auditoren sowie bezüglich eines möglichen Nachweises der Ausübung von Kontrollpflichten finden lassen.

WAS
genau soll zertifiziert werden?

WIE
werden die Schwerpunkte
für die Prüfung festgelegt?

WELCHE
Aussagekraft soll das
Ergebnis der Zertifizierung haben?

WER
und mit welchen Kompetenzen
wird die Zertifizierung durchführen?

DIE VORTEILE EINER UNABHÄNGIGEN ZERTIFIZIERUNG

1. **Vertrauensbildung** gegenüber Kunden, Beschäftigten, Lieferanten und Geschäftspartnern
2. **Wettbewerbsvorteil** durch höhere Akzeptanz der eigenen Leistungen
3. **Haftungsbegrenzung** für die Leitungsorgane
4. **Dokumentierter Nachweis** der rechtmäßigen Verarbeitung personenbezogener Daten
5. **Risikominimierung** des Eintretens von Datenschutzvorfällen
6. Erkennen datenschutzspezifischer **Optimierungspotentiale**
7. Steigerung der **Kundenzufriedenheit**
8. Steigerung der **Motivation der Beschäftigten** durch aktive Beteiligung
9. **Positive Risikobewertung** durch Prüfer oder Versicherungen

MOTIVATION

„Der Zertifizierungsprozess sollte den Unternehmensdatenschutz in seiner Gesamtheit abbilden“

Die seitens der AOK PLUS - Die Gesundheitskasse für Sachsen und Thüringen formulierte Motivation, sich einer externen und unabhängigen Auditierung der eigenen Verarbeitung von personenbezogenen Daten freiwillig zu unterziehen, wurde in der Aussage „Der Zertifizierungsprozess sollte den Unternehmensdatenschutz in seiner Gesamtheit abbilden“ treffend zusammengefasst.

Durch die Freiwilligkeit sich einer „Third Party Inspection“ zu unterziehen, demonstriert die AOK PLUS den eigenen Willen zu größtmöglicher Transparenz gegenüber Dritten für einen vertrauensvollen Umgang mit den bereitgestellten personenbezogenen Daten und bekräftigt zudem das in die AOK PLUS gesetzte Vertrauen für die Einhaltung der datenschutzrechtlichen Vorgaben.

Entscheidung für den Datenschutzstandard „DGI-DSM (DGI®)“

Die in der Evaluation des Projekts getroffene Aussage durch die AOK PLUS spezifizierte im weitesten Sinne unmittelbar die Kriterien für die Beauftragung einer Zertifizierung des eigenen Datenschutzniveaus.

Die AOK PLUS entschied sich für die Zertifizierung durch die DGI Deutsche Gesellschaft für Informationssicherheit AG gemäß des Datenschutzstandards DGI-DSM (DGI®).

Der Datenschutzstandard DGI-DSM (DGI®) stellt als Anforderung insbesondere das gesamte, ganzheitlich zu betrachtende, Management des Datenschutzes in den Mittelpunkt. Neben der obligatorischen Prüfung von Dokumentationen und der Beobachtung von Arbeitsabläufen liegen Prüfschwerpunkte des Standards vor allem auf der Integration der Aufbau- und Ablauforganisation sowie der Integration der Prozesse und Schnittstellen der Datenschutzorganisation in die Geschäftsprozesse.

Die Motivation der AOK PLUS zur freiwilligen Selbstkontrolle

BETEILIGTE DER ZERTIFIZIERUNG

Die in den Prozess einer Datenschutzzertifizierung involvierten Parteien und Stakeholder sind vielfältig und vertreten unterschiedliche Interessen.

Zum einen ist es unerlässlich den Gesetzgeber verlässlich zu interpretieren, um die datenschutzrechtlichen Anforderungen in vollem Umfang erfüllen zu können.

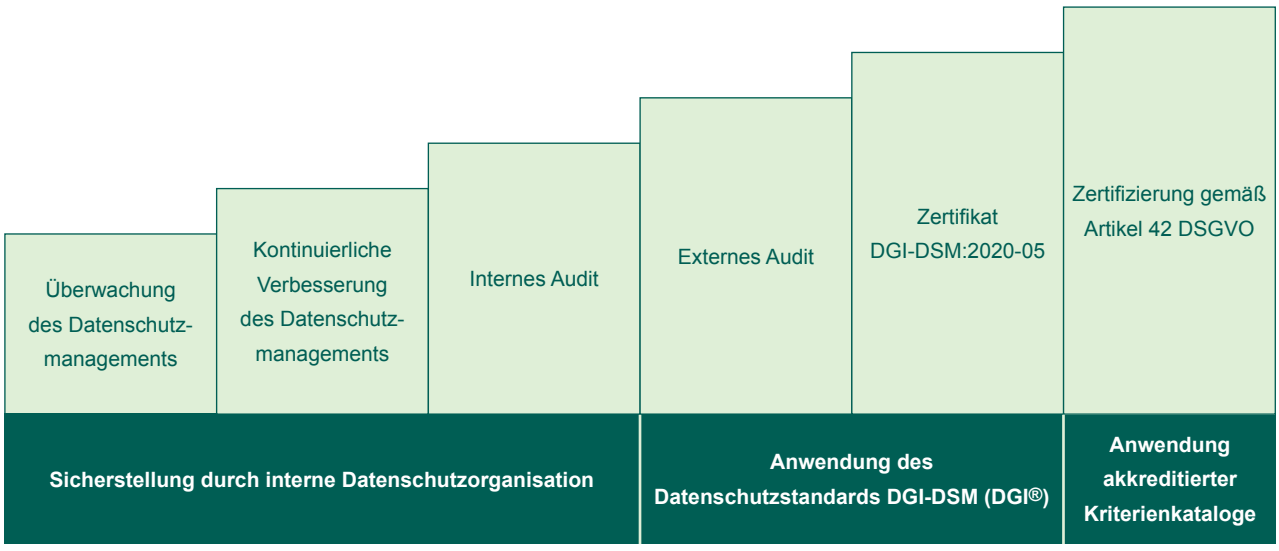
Auf der anderen Seite stehen die Wünsche und Anforderungen der Kunden, der Geschäftspartner sowie der Beschäftigten, die Gesetzestreue und einen verantwortlichen Umgang bei der Verarbeitung personenbezogener Daten einfordern.

Um für alle Seiten die erforderliche Transparenz bei der Einhaltung der datenschutzrechtlichen Vorgaben zu schaffen, stellt die DGI AG den Datenschutzstandard DGI-DSM (DGI®) als Zertifizierungsstandard sowie die “DGI-DSM:2020-05 - Umsetzungshinweise” als verbindlichen Prüfkatalog zur Verfügung, um objektive Kriterien für eine Vergleichbarkeit und Bewertung des Datenschutzniveaus zu liefern.

So gilt es durch die Geschäftsführung in Zusammenarbeit mit der internen Datenschutzorganisation die wesentlichen datenschutzrechtlichen Anforderungen herauszustellen. Die hierbei eruierten Prüfpunkte und zu präferierenden Audittätigkeiten sollten in das Auditprogramm einfließen, welches in enger Abstimmung zwischen der internen Datenschutzorganisation und dem Zertifizierer festgelegt werden muss.

Die Datenschutzzertifizierung durch fachkundige, unabhängige Dritte ermöglicht den verantwortlichen Personen die Ausübung der wahrzunehmenden Kontrollpflichten und kann gegenüber Dritten, durch den erfolgreichen Erwerb des Datenschutzzertifikats,die erforderliche Nachweispflicht sicherstellen.

Der Datenschutzstandard DGI-DSM (DGI®) orientiert sich an den Vorgaben des European Data Protection Board sowie der Datenschutzkonferenz, um auf die Anforderungen einer Zertifizierung gemäß Artikel 43 Absatz 3 DSGVO vorzubereiten.



Beteiligte der Zertifizierung

ZERTIFIZIERUNGSPROZESS

Der Zertifizerungsprozess führt in 5 Schritten zum Datenschutzzertifikat und ermöglicht neben der Überwachung und Aufrechterhaltung zusätzlich die kontinuierliche Weiterentwicklung sowie die Verbesserung des bereits umgesetzten Datenschutzniveaus.

1. Bestandsaufnahme

Bei der Bestandsaufnahme steht die Bewertung des aktuell umgesetzten Datenschutzniveaus im Vordergrund. Mit der Durchführung von internen oder externen Audits können die erforderlichen Prüfschritte vollzogen und die erforderlichen Informationen erhoben werden.

2. Beauftragung der Zertifizierung

Die Festlegung des zu zertifizierenden Bereichs, des Verfahrens, des Prozesses oder der Dienstleistung, für die das Datenschutzzertifikat erworden werden soll, bildet die Planungsgrundlage der zu auditierenden Dokumente, der Arbeitsweisen und der Infrastruktur.

3. Feststellung der Zertifizierungsreife

Die Überprüfung der Maßnahmenumsetzung bei der Verarbeitung von personenbezogenen Daten ermöglicht die Bewertung der Wirksamkeit der umgesetzten datenschutzrechtlichen Regelungen.

4. Erlangung Ihres Datenschutzzertifikats

Der erfolgreiche Nachweis der Erfüllung der Anforderungen des Datenschutzstandards DGI-DSM (DGI®) ermöglicht den Erwerb des Datenschutzzertifikats. Das Datenschutzzertifikat dient als Nachweis über die Einhaltung der an das Unternehmen gestellten datenschutzrechtlichen Vorgaben.

5. Aufrechterhaltung Ihrer Zertifizierung

Überwachungsaudits und Rezertifizierungsaudits sorgen für die Aufrechterhaltung und die kontinuierliche Verbesserung des etablierten Datenschutzniveaus.

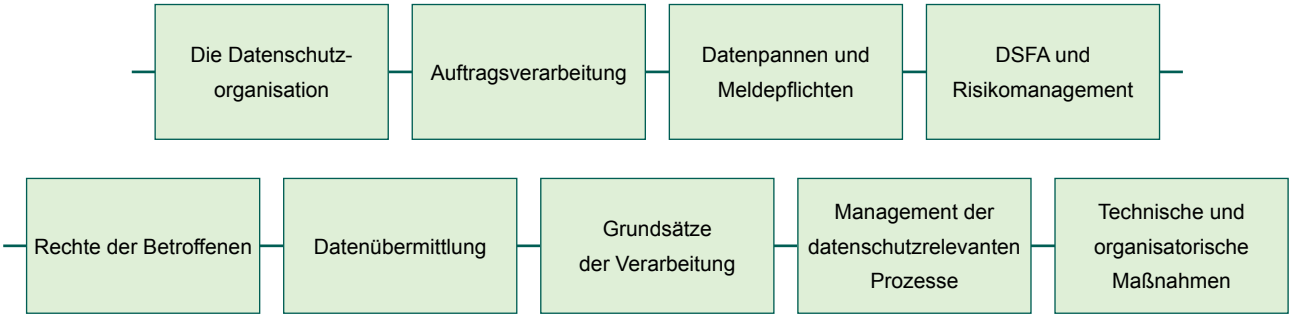
In 5 Schritten zum Datenschutzzertifikat

ABLAUF DER ZERTIFIZIERUNG

Die Auditdokumentation mit Auditplan, Auditchecklisten, Auditprotokollen, Auditbericht, Abweichungsdokumentation und Konformitätsnachweisen bildete die Grundlage für die Durchführung und Bewertung des Zertifizierungsaudits.

Im Rahmen des Audits bei der AOK PLUS wurde vor Ort überprüft, wie die Vorgaben aus der existierenden Dokumentation des Datenschutzmanagements der AOK PLUS sowie die daraus resultierenden internen Regelungen für die Einhaltung der datenschutzrechtlichen Pflichten in die Praxis umgesetzt wurden und wie die Wirksamkeit der umgesetzten Maßnahmen zu bewerten ist.

Die in der Auditcheckliste konkretisierten Prüfpunkte, die sich aus dem gemeinsam zwischen der AOK PLUS und der DGI AG festgelegten Anwendungsbereich (Scope) sowie der Stakeholderanalyse ergeben haben, wurden durch den Auditor bezüglich der Wirksamkeit der getroffenen Maßnahmen bewertet.



Prüfpunkte des Datenschutzstandard DGI-DSM (DGI®)

Die exemplarisch festgelegten Prüfpunkte, wie die Umsetzung technischer und organisatorischer Maßnahmen unter Berücksichtigung des Stands der Technik und insbesondere der Pseudonymisierung und Verschlüsselung personenbezogener Daten, sollten ein authentisches Abbild der alltäglichen Verarbeitungsprozesse in der AOK PLUS wiedergeben. Weitere Schwerpunkte der Auditierung waren die stichprobenhafte Prüfung der Einhaltung der Wahrung der Rechte der Betroffenen, die Einhaltung der Pflichten bei der Auftragsverarbeitung oder die Gewährleistung des angemessenen Schutzniveaus unter Zuhilfenahme der Durchführung von Datenschutzfolgeabschätzungen (DSFA).

ABLAUF DER ZERTIFIZIERUNG

Das bestehende hohe Datenschutzniveau der AOK PLUS zeichnete sich insbesondere dadurch aus, dass die regelmäßigen Aktivitäten des Datenschutzbeauftragten und des Datenschutzteams eindeutig dazu beitragen, ein sehr hohes Verständnis sowie eine sehr hohe Akzeptanz für die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Verarbeitung personenbezogener Daten innerhalb der gesamten Belegschaft erzeugen.

Das permanente Wirken der AOK PLUS das etablierte Datenschutzniveau kontinuierlich und nachhaltig zu steigern sowie das Management der Datenschutzorganisation ganzheitlich auf sämtliche Geschäftsaktivitäten auszurichten führt zunehmend zu einer äußerst positiven Resonanz bei allen beteiligten Parteien.

Das hervorragende Fachwissen und die langjährige Erfahrung der verantwortlichen Personen in der Datenschutzorganisation sichert vollständig die Erfüllung der Anforderungen des eng definierten Verarbeitungszwecks der personenbezogenen Daten bei der AOK PLUS.

Sämtliche gestellten Anforderungen an das Management der Datenschutzorganisation der AOK PLUS konnten abschließend als „im hohen Maße erfüllt“ bewertet werden.

Im Ergebnis wurden während des Audits keine Haupt- und Nebenabweichungen festgestellt. Somit wurde die erfolgreiche Erteilung des Zertifikates „Zertifizierter Datenschutz (DGI®)“ attestiert.

Der Auditbericht liefert der AOK PLUS eine ausführliche Darstellung der Feststellungen sowie Schlussfolgerungen zu den Auditkriterien und Prüfpunkten. Des Weiteren zeigt der Auditbericht die möglichen Verbesserungs- und Optimierungspotentiale des Managements der Datenschutzorganisation auf.

Kategorie	Beschreibung
Hauptabweichung	Gefährden den Erfolg des Datenschutzmanagements erheblich und führen zur Ablehnung eines Zertifikats
Nebenabweichung	Gefährden den Erfolg des Datenschutzmanagements teilweise und führen zur Erteilung eines Zertifikats unter Auflagen
Empfehlung zur Verbesserung	Gefährden den Erfolg des Datenschutzmanagements nicht wesentlich und schränken die Erteilung eines Zertifikats nicht ein

Bewertungsschema der Feststellungen

STATUS QUO

Der anfangs definierte Nutzen einer Datenschutzzertifizierung der AOK PLUS, eine objektive externe Sicht auf das eigene Handeln und eine Bewertung der Reife des eigenen Handelns zu bekommen, konnte abschließend vollumfänglich als erfüllt angesehen werden.

Die Kommentare und Reaktionen aller involvierten Parteien, insbesondere des Vorstands, der Führungsebenen, der Beschäftigten und der internen Revision sowie dem Sächsischen Staatsministerium für Soziales und Gesellschaftlichen Zusammenhalt als zuständige Fachaufsicht, waren ausnahmslos positiv und bestätigten die breite Akzeptanz für das erlangte Datenschutzzertifikat „Zertifizierter Datenschutz (DGI®)“.

Die hohe positive Resonanz, die positiven Erfahrungen aus dem Auditprozess und die Erlangung der Zertifizierung stehen als besondere Motivation, die Empfehlungen zur Verbesserung der Datenschutzorganisation in der AOK PLUS aufzunehmen und in die bestehenden Prozesse und Abläufe zu integrieren.

Die Datenschutzorganisation selbst begrüßte das gesamte Audit- und Zertifizierungsverfahren, das es ein, im Wortlaut, „unbequemes Thema“ für alle involvierten Parteien deutlich transparenter und den eigenen Anspruch an die Einhaltung interner Qualitätsnormen sichtbar machte.

Zudem erleichtern die Erlangung sowie die Aufrechterhaltung des Datenschutzzertifikats zukünftig den Nachweis der Wahrnehmung der geforderten Kontrollpflichten entscheidend.

Um das etablierte Datenschutzniveau der AOK PLUS aufrechtzuerhalten, müssen bis zum Rezertifizierungsaudit regelmäßige Überwachungsaudits durchgeführt werden.

Die innerhalb der dreijährigen Gültigkeit nach der Erst-Zertifizierung durchzuführenden jährlichen Überwachungsaudits sowie ein alle drei Jahre für die Rezertifizierung erforderliches Audit fordern von der AOK PLUS die kontinuierliche Verbesserung und Aufrechterhaltung des Managements der Datenschutzorganisation.

So sichert die begrenzte Gültigkeit den Stakeholdern eine gewisse Aktualität der umgesetzten Maßnahmen zum Management der Datenschutzorganisation zu.

AUSBLICK

Als sicher gilt, dass die Bedeutung von Datenschutzzertifizierungen aktuell und in Zukunft weiter zunehmen werden. Dies ist vor allem das Ergebnis der stärkeren Bewusstheit des Einzelnen, dass jede natürliche Person bei der Verarbeitung personenbezogener Daten die Wahrung der eigenen Rechte einfordern kann.

Zudem nimmt, aufgrund der Digitalisierung und der damit einhergehenden permanenten Erhebung und Übermittlung personenbezogener Daten, die Verarbeitung wie auch der Missbrauch in starkem Maße zu.

Dies wiederum führt vermehrt zur Nachfrage nach Zertifizierungen, um den Unternehmen, neben der unerlässlich gewordenen Transparenz beim Umgang mit personenbezogenen Daten, zusätzlich Wettbewerbsvorteile im eigenen Marktumfeld zu verschaffen.

Schlussendlich wird zertifizierten Unternehmen von Kunden per se ein höheres Vertrauen eingeräumt, als es nicht zertifizierten Unternehmen gegenüber entgegengebracht wird.

ÜBER DIE AOK PLUS

Die AOK PLUS – Die Gesundheitskasse für Sachsen und Thüringen ist ein Träger der gesetzlichen Krankenversicherung aus der Gruppe der Allgemeinen Ortskrankenkassen und eine Pflegekasse für die Länder Sachsen und Thüringen.

Die Zentrale der AOK PLUS hat ihren Sitz in Dresden. Sie verfügt über mehr als 140 Filialen in Sachsen und Thüringen. Rund 7000 Mitarbeiter betreuen die über 3 Millionen Versicherten.

Ansprechpartner für die Durchführung des Projekts ist auf Seiten der AOK PLUS

Herr Dirk Schmidt
- Datenschutzbeauftragter -
Telefon 0800 10590 - 14100
E-Mail Datenschutz@plus.aok.de

ÜBER DIE DGI AG

Die DGI Deutsche Gesellschaft für Informationssicherheit AG, mit Sitz in Berlin, ist die Dachmarke der Geschäftsbereiche Beratung und Weiterbildung. Zu den Schwerpunkten zählen die Begleitung der Umsetzung von Datenschutz- und Informationssicherheitmanagementsystemen sowie deren Zertifizierungen.

Die Akademie der DGI Deutsche Gesellschaft für Informationssicherheit AG ist einer der führenden Bildungsdienstleister bei der Ausbildung in den Bereichen Informationssicherheit, Datenschutz, Business Continuity sowie IT Risikomanagement.

Ansprechpartner für die Durchführung des Projekts ist auf Seiten der DGI AG

Herr Ronny Neid
- Vorstand -
Telefon +49 30 31 51 73 89 - 10
E-Mail info@dgi-ag.de