Detaillierte Begutachtungsergebnisse

Auditbericht 2024

Informationssicherheits- und Datenschutzmanagementsystem ISO/IEC 27001:2022 und ISO/IEC 27701:2019

für

DATEV eG

Paumgartnerstr. 6 - 14

D – 90429 Nürnberg

Hauptstandort mit allen dazugehörigen Standorten

CIS - Certification & Information Security Services GmbH

Headquarters

1010 Vienna, Salztorgasse 2/3/7

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

Inhaltsverzeichnis

1. Erläuterungen zur Begutachtung

1.1 Ausgangslage

Norm-Referenzen ISO/IEC 27001/27701: 4/5.2 Kontext der Organisation

Laut veröffentlichten Kurzprofil der DATEV eG ist sie der drittgrößte Anbieter für Business Software in Deutschland (IDC-Ranking 2023 und einer der großen europäischen IT-Dienstleister).
Mit Sitz in Nürnberg stellt die DATEV eG mit Software, Cloud-Lösungen und Know-how die Basis für die digitale Zusammenarbeit zwischen dem Mittelstand und den steuerlichen Beraterinnen und Beratern bereit, die sich um die betriebswirtschaftlichen Belange der Betriebe kümmern. Über diese Community unterstützt die DATEV eG insgesamt 2,8 Millionen Unternehmen, Selbstständige, Kommunen, Vereine und Institutionen. Mit mehr als 8.900 Mitarbeiterinnen und Mitarbeitern begleitet das Unternehmen rund 620.000 Kunden als Partner mit Lösungsangeboten zur Digitalisierung ihrer kaufmännischen Prozesse. Informationssicherheit, Datenschutz und steuerliche Compliance haben dabei höchste Priorität.

Da Informationssicherheit und Datenschutz voneinander untrennbare Themenbereiche sind, verfolgt die DATEV eG einen integrierten Ansatz und hat ihr Informationssicherheits- und Datenschutz-Managementsystem (ISMS/DSMS) nach der ISO/IEC 27001:2022 und ISO/IEC 27701:2019 von der CIS - Certification & Information Security Services GmbH (nachfolgend CIS) zertifizieren lassen. Neben diesen Zertifikaten stehen weitere ISO/IEC-Zertifikate, wie für den Entsorgungs- oder für den Qualitäts- und Service-Managementprozess zum Abruf auf der Firmenwebseite zur Verfügung.

1.2 Zweck der Begutachtung

Ein Baustein für die Vertrauensbildung und Nachweisbarkeit des hohen Stellenwertes und der Wirksamkeit der getroffenen Maßnahmen zur Sicherstellung der Informations-sicherheit und des Datenschutzes ist die Bereitstellung der seit 2006 und 2010 erworbenen Zertifikate für das Datenschutz- und Informationssicherheits-Managementsystem auf www.datev.de/datenschutz. Die DATEV eG möchte ihren Mitgliedern und weiteren Kunden ermöglichen, den an sie gestellten Kontrollpflichten auf einfache und wirksame Weise nachkommen und auch etwaige Dokumentationspflichten gegenüber externen Stellen und Kontrollorganen hinsichtlich der Auswahl ihres Dienstleisters effektiv erfüllen zu können.

Mit einem freiwilligen Informationssicherheits- und Datenschutzaudit möchte die DATEV eG einheitlich und übergreifend aufzeigen, dass Informationssicherheit und Datenschutz in einem integrierten Managementsystem angemessen, wirksam und nachhaltig umgesetzt sind.

Ferner möchte die DATEV eG damit darlegen, dass die implementierten Prozesse sicherstellen, dass die Verarbeitungstätigkeiten bei der Planung, Umsetzung, Prüfung und kontinuierlichen Verbesserung zur Erreichung der Ziele Vertraulichkeit, Verfügbarkeit inkl. Belastbarkeit und Integrität gegenüber bestehenden Datenschutz- und Informationssicherheitsrisiken sicher und so gestaltet sind, dass sie den Grundsätzen der Verarbeitung personenbezogener Daten entsprechen.
Die DATEV eG möchte darüber hinaus darlegen, dass ihr Risikomanagementprozess sicherstellt, dass sowohl die Informationssicherheitsrisiken als auch die Datenschutzrisiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung ihrer Daten berücksichtigt werden.

Das Zertifikat bescheinigt auch, dass die Prozesse des integrierten ISMS/DSMS sicherstellen, dass die technischen und organisatorischen Maßnahmen angemessen und wirksam geplant, umgesetzt und aufrechterhalten werden.

1.3 Anwendungsbereich des Informationssicherheits- und Datenschutzmanagementsystems

Norm-Referenzen
ISO/IEC 27001/27701: 4.3/5.2.3 Festlegen des Anwendungsbereichs des ISMS/DSMS 4.4/5.2.4 Informationssicherheitsmanagementsystem/DSMS

Das Audit für die Begutachtung des Informationssicherheits- und Datenschutzmanagementsystems umfasst die DATEV eG mit allen Standorten in Deutschland. Dies beinhaltet die Softwareentwicklung, Datenverarbeitung, Erbringung von Service-, Schulungs- und Consultingleistungen, die im Scope befindlichen Rechenzentren sowie das Digital & Print Solution Center und die zum Prüfungszeitpunkt bestehenden 22 DATEV-Niederlassungen.
Die Auditkriterien bilden die Normforderungen der ISO/IEC 27001 in Kombination mit der ISO/IEC 27701 und der geforderten Erklärung zur Anwendbarkeit der DATEV: Statement of Applicability | Version 2.0 | 19.09.2024.

Das Statement of Applicability basiert auf den anzuwendenden Maßnahmen aus den Anhängen beider Normen und weisen keinerlei Ausschlüsse auf. Ferner fließen weitere interne und externe Anforderungen aus Verfahren, Anweisungen, Verträgen, etc., in die Auditkriterien ein.

Die Begutachtung der Standorte und Niederlassungen wurde im so genannten Stichprobenverfahren durchgeführt, bei dem jeweils gemäß Zertifizierungsregeln die Anzahl und Auswahl der zu begutachtenden Standorte für die Auditierung ermittelt wird.

Auf Grund einer ganzheitlichen Betrachtung hat die DATEV eG ein integriertes Managementsystem etabliert, dass sowohl organisatorische, technische und standortbezogene Gesichtspunkte vereint als auch nach innen auf Strukturen und Beschäftigte und nach außen auf Mitglieder, deren Mandanten, weitere Kunden und Geschäftspartner wirkt.

2. Beschreibung des integrierten IS-/DS-Managementsystems

2.1 Verantwortung der Leitung

Norm-Referenzen
ISO/IEC 27001/27701: 5.1/5.3 Führung und Verpflichtung 5.1/5.3.2 Politik 5.2/5.3.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation 6.2/5.4.2 Informationssicherheitsziele und Planung zu deren Erreichung

Der Vorstand der DATEV eG unterstützt das Informationssicherheits- und Datenschutzmanagementsystem durch die Freigabe der Strategie zu Informationssicherheit und Datenschutz und den dazugehörigen Directiven sowie über die Bereitstellung ausreichender Ressourcen. Das Informationssicherheits- und Datenschutzmanagementsystem ist vollständig in das Ziel- und Kontrollsystem der DATEV eG eingebunden. Über den regelmäßigen Bericht des Informationssicherheits- und Datenschutzbeauftragten erhält der Vorstand die Information über die Zielerreichung und aktuelle Themen. Der Vorstand ist entsprechend den Vorgaben an ein Managementsystem in bedeutende informations- und datenschutzrelevante Themen involviert. So werden wichtige Änderungen des IS-/DS-Managementsystems über Entscheidungsvorlagen durch den Vorstand behandelt und verabschiedet.

Die festgelegte Directive „Unternehmenssicherheit und Datenschutz" bietet übergeordnete Leitsätze mit DATEV-weiter Gültigkeit zur Planung, Umsetzung und ständigen Aufrechterhaltung der rechtlichen, regulatorischen, kundenorientierten und anderen Anforderungen.
Die Vorgaben zu Datenschutz und Unternehmenssicherheit sind im Security Privacy Framework (SPF) auf der Basis der Anforderungen der Normen, z. B. ISO/IEC 27001 und ISO/IEC 27701 in Policies und Standards dokumentiert.

Das integrierte Informationssicherheits- und Datenschutzmanagementsystem der DATEV eG verbindet die Aspekte und Forderungen der Normen ISO/IEC 27001 und ISO/IEC 27701 und den datenschutzspezifischen Vorgaben, aus den regulatorischen Anforderungen zum Datenschutz, insbesondere der Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz.

2.2 Risikomanagement

Norm-Referenzen
ISO/IEC 27001/27701: 6.1/5.4.1 Maßnahmen zum Umgang mit Risiken und Chancen 6.1.2/5.4.1.2 Informationssicherheitsrisikobeurteilung 6.1.3/5.4.1.3 Informationssicherheitsrisikobehandlung

Das Risikomanagement in der ISO/IEC 27001 bzw. ISO/IEC 27701 ist ein zentraler Bestandteil des Datenschutz- und Informationssicherheitsmanagementsystems und dient dazu, Risiken für die Informationssicherheit und den Datenschutz systematisch zu identifizieren, zu bewerten und angemessen zu behandeln. Der Prozess beginnt mit der Identifikation von Risiken, wobei Organisationen ihre Werte (Assets), Bedrohungen und Schwachstellen analysieren müssen. Diese Risiken werden anschließend anhand ihrer Eintrittswahrscheinlichkeit und potenziellen Auswirkungen bewertet, um eine Priorisierung vorzunehmen.

Basierend auf dieser Bewertung erfolgt die Risikobehandlung, die verschiedene Strategien umfasst: Risiken können durch technische oder organisatorische Maßnahmen reduziert, auf Dritte übertragen (z. B. Versicherungen), akzeptiert oder vermieden werden. Die Auswahl geeigneter Maßnahmen erfolgt unter Berücksichtigung der Maßnahmen aus dem Anhang der Normen sowie weiterer regulatorischer und geschäftlicher Anforderungen.

Ein wesentlicher Bestandteil des Risikomanagements ist zudem die regelmäßige Überprüfung und Verbesserung. Risiken ändern sich aufgrund neuer Bedrohungen, technologischer Entwicklungen oder veränderter Geschäftsprozesse. Daher muss das Risikomanagement kontinuierlich angepasst und aktualisiert werden, beispielsweise durch regelmäßige Risikobewertungen und Audits. Durch diesen systematischen Ansatz kann erreicht werden, dass Organisationen ihre Informationssicherheitsrisiken proaktiv steuern und ihre Widerstandsfähigkeit gegenüber Cyber-Bedrohungen und Sicherheitsvorfällen erhöhen.

Das Vorgehen der DATEV zur Identifikation, Bewertung und Behandlung von Risiken in der Informationssicherheit und im Datenschutz erfolgt über einen etablierten Risikomanagementprozess. Dieser gilt für alle Services – unabhängig davon, ob eine Verarbeitung personenbezogener Daten erfolgt oder andere schützenswerte Daten und Informationen.

Vorgelagert zum eigentlichen Informationssicherheits-/Datenschutz-Risiko-Assessment ist bei Services, die personenbezogene Daten verarbeiten, die Meldung der relevanten Angaben zur Führung des Verzeichnisses der Verarbeitungstätigkeiten (VVT) erforderlich. Diese Meldung erfolgt über den toolgestützten Risk2Value (R2V)-Prozess, der die strukturierte Erfassung, Bewertung und Überwachung von Risiken ermöglicht. Jeder verantwortliche Mitarbeiter, darunter Produkt- oder Serviceowner sowie verantwortliche Führungskräfte, ist verpflichtet, eine Datenschutz-IDV-Meldung für das VVT zu erstellen und regelmäßig ein Risk Assessment durchzuführen. Die Meldungen erfolgen über Risk2Value (R2V) und beinhalten verschiedene Schritte. Zunächst wird ein Meldeformular ausgefüllt, das entweder manuell erstellt oder durch den Import eines Servicekatalog-Eintrags generiert werden kann. Das Formular enthält allgemeine Angaben zur Verarbeitung, eine Beschreibung der verarbeiteten Daten, weiterführende Informationen zur Meldung, eine DSFA-Abschätzung (Datenschutz-Folgenabschätzung), Anmerkungen zum Datenschutz, Aktivitätslinks, Dokumentationen sowie eine Übersicht über den gesamten Verlauf des Prozesses.

Nach der Meldung erfolgt ein toolgestütztes Risiko-Assessment, in dem die Eintrittswahrscheinlichkeit und Schadenshöhe von Informationssicherheits- und Datenschutz-Risiken anhand der elementaren Gefährdungen des BSI sowie der daraus abgeleiteten Datenschutz-Gefährdungen der DSGVO bewertet werden. Abhängig von der Relevanz-Prüfung zur Durchführung einer DSFA wird diese, sofern erforderlich, projektorientiert anhand detaillierter Arbeitshilfen umgesetzt. Im Rahmen des Kontroll-Assessments wird geprüft, welche Sicherheitsmaßnahmen aus dem Security Privacy Framework in Abhängigkeit vom Asset-Typ und Schutzbedarf umgesetzt werden müssen. Diese Auswahl und Umsetzung werden dokumentiert, wobei der Serviceowner für die Durchführung der Maßnahmen verantwortlich ist. Die abschließenden Schritte umfassen die Qualitätssicherung sowie die Bearbeitung des Freigabeformulars, mit dem entweder die Freigabe akzeptiert oder eine Risikoübernahme beschlossen wird.

2.3 Informationssicherheits- und Datenschutzrichtlinien

Norm-Referenzen
ISO/IEC 27001/27701: 7.5/5.5.5 Dokumentierte Information A.5.1 Informationssicherheitspolitik und -richtlinien

Die Gestaltung von Verarbeitungsprozessen personenbezogener Daten erfolgt unter Anwendung der Vorgaben aus dem Security Privacy Framework (SPF) sowohl für die Verarbeitung als Verantwortlicher als auch im Auftrag methodisch unter Berücksichtigung der umzusetzenden Maßnahmen.
Im Fokus steht die Behandlung der Informationssicherheits- und Datenschutzrisiken zur Gewährleistung eines sicheren Betriebs und die Einhaltung der von der DS-GVO vorgesehenen Grundsätze der Verarbeitung wie Rechtmäßigkeit und Transparenz.

Zur Sicherstellung der Betroffenenrechte wie Auskunft, Berichtigung, Löschung, Einschränkung, Übertragung und Widerspruch sind entsprechende Prozesse definiert, die unter anderem die Identifikation des Betroffenen, die Einhaltung der Fristen, die Einbindung zuständiger Mitarbeiter und die Nachweisführung beinhalten. Der Umgang mit Informationssicherheits- und Datenschutzvorfällen wird prozessual gesteuert. Dazu gehören verschiedene Subprozesse, die festlegen, wie die Meldung innerhalb der DATEV eG bei Auftritt eines möglichen Vorfalls, die Meldung an die Aufsichtsbehörde von Vorfällen mit Datenschutzrelevanz innerhalb der vorgegebenen Frist und die Benachrichtigung von Betroffenen zu erfolgen hat.

2.4 Interne und externe Kommunikation

Norm-Referenzen
ISO/IEC 27001/27701: 7.4/5.5.4 Kommunikation

Zentrales Element des Informationssicherheits- und Datenschutzmanagementsystems ist die interne und externe Kommunikation. Im Rahmen der jährlichen Vermarktungs- und Vertriebsplanung werden die Maßnahmen des Kommunikations- und Vermarktungskonzept festgelegt. Ziel ist es, Informationen über die aktuelle Sicherheitslage und Maßnahmen zur Sensibilisierung an die jeweilige Zielgruppe zu geben. Dafür stehen zahlreiche Kommunikationsmedien zur Verfügung.

Intern sind insbesondere Unternehmen-News, Fachbereich-News, Datenschutz-Blog, Informationsveranstaltungen, Schulungen, Directiven und Leitfäden zu nennen. Kommunikationsbedarf zu externen Stakeholdern besteht zu allen Mitgliedern, Kunden, Mandanten und anderen interessierten Parteien, der über das DATEV-Magazin mit Schwerpunktthemen, der Blog in Kooperation mit dem DiFü (digitaler Führerschein), das Trialog-Magazin, Veranstaltungen, Messen und Kongresse usw. erfüllt wird.

Der Internetauftritt der DATEV bietet Mitglieder und Interessierten umfassende Informationen zu den Produkten und Services der DATEV. Die Webseiten ‚Datenschutz und Datensicherheit bei DATEV' umfassen zahlreiche Informationen zu den Datenschutzprinzipien bei DATEV, zu Auftragsverarbeitungsvereinbarungen, technisch-organisatorischen Maßnahmen sowie Datenschutz-Steckbriefe und detaillierte Leistungsbeschreibungen der DATEV Produkte inkl. der jeweiligen Regelungen zur Auftragsverarbeitungen und vieles mehr.

2.5 Dokumentenmanagement

Norm-Referenzen ISO/IEC 27001/27701: 7.5/5.5.5 Dokumentierte Information

Das Organisationshandbuch (OHB), eine Sammlung von Organisationsanweisungen, wurde durch das DATEV Set of rules, dem neuen verbindlichen Regelwerk der DATEV eG abgelöst. Es handelt sich um ein abgestuftes Verfahren der Regelsetzung, das zwischen Code of Business Conduct, Directiven, Policies und Standards unterscheidet.

Die übergeordneten Leitsätze zu Unternehmenssicherheit und Datenschutz sowie Datenethik sind als Dokumente in Form von Directiven geregelt. Hingegen sind die Inhalte von Policies und Standards, abgeleitet aus Normen, Gesetzen und internen Vorgaben, toolgestützt über eine SharePoint-Lösung, dem Security Privacy Framework (SPF), abgebildet. Das SPF stellt den verbindlichen Handlungsrahmen für alle Mitarbeitenden der DATEV eG dar und ist von diesen in ihrem Aufgabengebiet entsprechend dem risikoorientierten Vorgehen umzusetzen.

Im Zuge der Neustrukturierung wurden die ursprünglichen OHB-Regelungen den Verantwortlichen in den Fachbereichen zugewiesen und von diesen auf Relevanz und Aktualität geprüft. Anschließend erstellten die Fachverantwortlichen die Standards, unterstützt durch Schulungsmaterial. Der Freigabe-Prozess dieser Standards sieht eine inhaltliche Abstimmung mit dem Verantwortlichen der Domäne des Regelungs-bereichs sowie eine Genehmigung eines weiteren Verantwortlichen im entsprechenden Fachbereich vor.

Diese qualitätssichernden Maßnahmen sorgen für ein schlüssiges und konsistentes Vorgaben-Rahmenwerk.

2.6 Planung und Steuerung der Informationssicherheits- und Datenschutzprozesse

Norm-Referenzen
ISO/IEC 27001/27701: 8.1/5.6.1 Betriebliche Planung und Steuerung

Das Informationssicherheits- und Datenschutzmanagementsystem führt die Verantwortlichkeiten, Ressourcen, Prozesse und Methoden zur Einhaltung der Anforderungen aus dem Informationssicherheits- und Datenschutzbereich in eine homogene Struktur und ermöglicht so eine transparente und systematische Planung, Durchführung und kontinuierliche Verbesserung der Abläufe. Die definierten Vorgaben aus dem Security Privacy Framework sind in die Gestaltung der Prozesse und deren betriebliche Umsetzung eingeflossen.

2.7 Organisation der Informationssicherheit und des Datenschutzes

Norm-Referenzen
ISO/IEC 27001/27701: 5.3/5.3.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation A.5.2 Informationssicherheitsrollen und -verantwortlichkeiten A.5.3 Aufgabentrennung A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung A.7 Physische Maßnahmen

2.7.1 Three-Lines-of-Defense-Modell

Die DATEV eG verfolgt das Modell der drei Verteidigungslinien zur systematischen Herangehensweise an Risiken, die im Unternehmen auftreten können. Diese müssen frühzeitig erfasst, identifiziert, analysiert und bewertet, sowie innerhalb der Unternehmung kommuniziert werden.

Die 1st-Line besteht aus den für die laufende Beratung der Fachbereiche zuständigen Teams der operativen IT-Security und Privacy. Sie werden durch die Bereichs-beauftragten für Datenschutz, Datenschutzkoordinatoren und Security Engineers unterstützt.

Die 2nd-Line ist als Governance-Einheit für die Erstellung von Vorgaben und die Durchführung von internen Audits zur Überwachung und Unterstützung der 1stLine zuständig. Die Governance-Einheit besteht aus den Teams Strategy & Certifications und Management Systems & Governance.
Die 3rd-Line wird durch die Revision wahrgenommen. Sie überwacht als unabhängige Instanz das Risikomanagement.

Ein Datenschutzbeauftragter (DSB) ist im Rahmen der Wahrnehmung seiner Datenschutzaufgaben unabhängig tätig und bestellt worden. Aufgrund der thematischen Nähe und der damit verbundenen Integration der Managementsysteme für Informationssicherheit und Datenschutz nimmt er zugleich die Rolle des Informationssicherheitsbeauftragten (ISB) wahr. In seiner Doppelrolle erarbeitet und schult er Vorgaben, kontrolliert deren Umsetzung und nimmt die zentrale Steuerung für alle Informationssicherheits- und Datenschutzmanagementprozesse wahr.

Der Informationssicherheits- bzw. Datenschutzbeauftragte wird bei der Erfüllung seiner Aufgaben von kompetenten, hauptamtlichen Mitarbeitenden und von zahlreichen weiteren Datenschutz-, Sicherheits- und Kontrollorganen des Hauses unterstützt. Dazu gehören beispielsweise das Gesamtsicherheitsgremium, die Bereichsbeauftragten für Datenschutz oder die Physische Sicherheit. Die besondere Stellung des Informationssicherheits- bzw. Datenschutzbeauftragten aus Sicht der DATEV eG wird unter anderem durch seine Zugehörigkeit zum Kreis der leitenden Angestellten dokumentiert.

2.7.2 Organisation der DATEV-Niederlassungen

Die DATEV-Niederlassungen werden hinsichtlich der Informationssicherheit und des Datenschutzes nach zentralen Vorgaben gelenkt. Dazu gehört u. a. die Festlegung der Informationssicherheits-/Datenschutzpflichten und -aufgaben.
Im Geltungsbereich der auf www.datev.de veröffentlichten technischen und organisatorischen Maßnahmen sind alle Niederlassungen eingeschlossen. Eine zentrale Rolle kommt der Leitung der jeweiligen Niederlassung zu. Sie ist für den Betrieb und die Sicherheit einer oder mehrerer Niederlassungen verantwortlich.

Die Regelungen zu Informationssicherheit und Datenschutz für Niederlassungen sind in den Vorgaben des Security und Privacy Frameworks (SPF) beschrieben. In Niederlassungen finden grundsätzlich alle Regelungen analog zu den Standorten der DATEV in Nürnberg Anwendung. Niederlassungsspezifische Ausprägungen für die Niederlassungsleitung und -mitarbeitende sind entsprechend im SPF definiert. Alle Mitarbeitende, die Niederlassungen besuchen bzw. darin arbeiten, müssen sich mit den jeweils vor Ort abweichend geltenden Regelungen vertraut machen.

Die Vorgaben zur physischen Sicherheit in den Niederlassungen umfassen die Themenfelder Zutrittskontrolle, Besuche, Technikraum und Brandschutz.

Der Zutritt in der Niederlassung ist zwischen Schulungsbereich und internem Bereich geteilt. Der Zutritt zum internen Bereich wird durch physische Sicherheitsmaßnahmen eingeschränkt und u. a. durch Video überwacht. Im Schulungsbereich werden keine vertraulichen Informationen oder personenbezogene Daten verarbeitet.

Mitarbeitende in den internen Bereichen der Niederlassungen MÜSSEN die Identifikation aller Besucher:innen überprüfen und dokumentieren. Dabei müssen sich alle Besucher:innen durch ein gültiges, amtliches Lichtbilddokument ausweisen. Die besuchte Person hat die Pflicht, die Besucher:innen am Empfang oder am Eingang der Niederlassung bzw. des internen Bereichs der Niederlassung abzuholen oder abholen zu lassen und eine kurze Sicherheitsunterweisung durchzuführen.
Während des gesamten Aufenthalts innerhalb des internen Bereiches der DATEV Niederlassung besteht Begleitpflicht.

Technikräume in Niederlassungen sind explizit als Sicherheitsbereiche ausgewiesen und durch ein technisches Zutrittssystem abgesichert, das über den zentralen Betriebsschutz in Nürnberg gesteuert wird. Ein Zutritt ist nur durch dedizierte Mitarbeiter möglich, wie den Sicherheitsbeauftragten der Niederlassung, und wird beim Betriebsschutz angemeldet und protokolliert.

Für die Sammlung und Entsorgung von Papierdatenträgern werden verschlossene Aluminiumbehälter eines externen Dienstleisters bereitgestellt. Ist die Füllhöhe der Sicherheitsbehälter erreicht, wird durch die Niederlassung die Abholung durch den Entsorgungspartner veranlasst. Der Transport der Sicherheitsbehälter wird in geschlossenen und GPS-überwachten Kofferfahrzeugen vorgenommen. Im Entsorgungsunternehmen erfolgt nach Passieren der Sicherheitsschleuse das Abkippen der Behälter und dabei die Öffnung, so dass das gesammelte Material ohne Einsicht durch Externe direkt der Schredderanlage zugeführt und vernichtet wird.

Die Auswahl, Prüfung und Kontrolle der Entsorgungspartner erfolgt zentralseitig. Ein Rahmenvertrag besteht für einen namhaften Entsorgungsfachbetrieb. Wesentliche Auswahlkriterien stellen Bescheinigungen und Zertifikate dar u. a. über die ISO 9001:2015 Qualitätsmanagement sowie die ISO 21964/DIN 66399 Prozess der Datenvernichtung.
Die Kontrolle umfasst eine jährliche Vor-Ort-Prüfung des Entsorgungspartners anhand einer Prüfliste und Standortbegehung zur Begutachtung der Gebäudesicherheit, Zutrittssystem usw.
Elektronische Datenträger zur Entsorgung fallen in den Niederlassungen selten an und werden durch die zuständigen Sicherheitsbeauftragten der Niederlassungen an die interne IT zur Entsorgung weitergegeben.

Das Prinzip des mobilen Arbeitens ist auf das Arbeiten in der Niederlassung gleichermaßen anwendbar. Zum Beispiel werden beim mobilen Arbeiten personenbezogene Daten im Auftrag grundsätzlich nur mit von DATEV zur Verfügung gestellten mobilen Endgeräten mit Remote-Anbindung an DATEV-Netze verarbeitet. Die Festplatten des mobilen Arbeitsplatz-Rechners sind vollverschlüsselt.
Der elektronische Transport von Daten an das Rechenzentrum erfolgt über eine verschlüsselte Verbindung mit Zwei-Faktor-Authentisierung.

Die jährliche Unterweisung der Mitarbeitenden in Bezug auf Brandschutzbestimmungen und dem Umgang mit Handfeuerlöschern sowie die Durchführung von Räumungsübungen sind fester Bestandteil des Brandschutzkonzeptes der Niederlassungen.

Die Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen werden durch themenspezifische Self-Assessments, die zentralseitig zur Verfügung gestellt werden, unterstützt.

Die Handhabung des Datenschutzes in der Niederlassung hat beispielgebende Funktion, weil die zahlreichen Schulungsteilnehmer hier die verschiedenen Datenschutz- und Sicherheitsmaßnahmen und ihr Zusammenspiel vor Ort erleben können.

2.8 Überwachung und Verbesserung

Norm-Referenzen
ISO/IEC 27001/27701: 9.1/5.7 Überwachung, Messung, Analyse und Bewertung 9.2/5.7.2 Internes Audit 10.1/5.8.2 Fortlaufende Verbesserung 10.2/5.8.1 Nichtkonformität und Korrekturmaßnahmen

Das integrierte Informationssicherheits- und Datenschutzmanagementsystem der DATEV eG unterliegt einem kontinuierlichen Überwachungs- und Verbesserungsprozess. Die Überwachung der IT-Systeme hinsichtlich ihrer sicheren und datenschutzkonformen Gestaltung steht dabei ebenso im Vordergrund wie die Informationssicherheits- und Datenschutzorganisation selbst.

Das Kennzahlensystem des integrierten Managementsystems (IMS) verfolgt das Ziel, eine fundierte Entscheidungsgrundlage für die Steuerung der Prozesse im IMS bereitzustellen. Zudem dient es der Überprüfung der Wirksamkeit der Steuerungsmaßnahmen sowie der Bewertung der Zielerreichung innerhalb des IMS. Dazu sind Kennzahlen in drei Kategorien eingestuft. Die Managementkennzahlen und Datenschutzkennzahlen unterliegen der Verantwortung der Abteilung Governance.

Unterstützungskennzahlen hingegen liegen in der Zuständigkeit der jeweiligen Fachabteilungen. Kennzahlen werden in Bezug auf den Abdeckungsgrad und die Effektivität erhoben wie unter anderem die Teilnehmerquote an Pflichtschulungen, die Aktualität von Richtlinien, die Sicherheit bei Softwareentwicklungsprojekten und das Management von Datenschutz- und Informationssicherheitsvorfällen.

Die Erstellung neuer Kennzahlen erfolgt entweder auf Basis einer Forderung der ISO/IEC 27001 und ISO/IEC 27701 zur Wirksamkeitsprüfung von Maßnahmen oder aufgrund eines internen Bedarfs. Mit der zuständigen Fachabteilung wird die neue Kennzahl abgestimmt, die erforderliche Datenbasis vorbereitet und ein Kennzahlensteckbrief erstellt. Die Erhebung der aktuellen Werte erfolgt in regelmäßigen Intervallen, sei es monatlich, vierteljährlich, halbjährlich oder jährlich.

Der Prozess der Kennzahlenverwaltung beginnt mit der Erhebung durch verantwortliche Mitarbeitende der entsprechenden Abteilungen. Anschließend erfolgt die Übermittlung der erfassten Daten und die Dokumentation im dafür vorgesehenen Confluence-Bereich. Anschließend werden die Kennzahlen von den dafür zuständigen Mitarbeitenden analysiert und anhand eines Ampelsystems bewertet. Sollte es zu Abweichungen von festgelegten Toleranzwerten kommen, wird der Datenschutz- und Informationssicherheitsbeauftragte involviert. Bei gravierenden Abweichungen wird das Gesamtsicherheitsgremium informiert. Je nach Ergebnis der Bewertungen werden Maßnahmen zur Prozessoptimierung, Fehlerreduktion oder Effizienzsteigerung erarbeitet und umgesetzt. Der Prozess der Kennzahlenverwaltung sieht zudem vor, die übermittelten Daten in Bezug auf die Effektivität der Kennzahl zu überprüfen und anzupassen.

Die Informationssicherheit und der Datenschutz werden fortlaufend im Rahmen eines jährlich festgelegten Audit-Programms durch die beschlossenen internen Audit-Maßnahmen durch die Abteilungen Privacy & Information Security und der IT-Revision überprüft.
Festgestellte Abweichungen oder Potenziale fließen in einen Verbesserungsplan ein, der regelmäßig aktualisiert und überwacht wird. Neben diesen mehrstufigen internen Kontrollen beauftragt die DATEV eG auch unabhängige, zertifizierte Gutachter und Zertifizierungsstellen mit externen Überprüfungen des Informationssicherheits- und Datenschutzmanagementsystems.

2.9 Allgemeine Informationssicherheits- und Datenschutzmaßnahmen (Technische und organisatorische Maßnahmen)

Die Priorität der Informationssicherheit und des Datenschutzes in Verbindung mit der Größenordnung der DATEV eG ermöglicht umfassende und effektive Informations-sicherheits- und Datenschutzmaßnahmen. Die DATEV eG hat im Rahmen ihres komplexen Sicherheitssystems sowohl in baulicher, personeller, organisatorischer als auch technischer Hinsicht alle wichtigen Vorkehrungen getroffen. Damit kann die hohe Sicherheit der IT--Infrastruktur, der Prozessumgebungen, des Datenbestandes sowie des Betriebsablaufs gewährleistet werden.

Eine Vielzahl von Vorgaben und Maßnahmen, die sich über die Verteilung, den Transport, die Aufbewahrung bis hin zur Entsorgung oder den Versand von Daten und Informationen erstrecken, dient dem Ziel, einen unbefugten Zugriff und den ordnungsgemäßen Umgang sicherzustellen.

Die DATEV eG stellt ihren Kunden und interessierten Parteien ihre allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Verfolgung der Datenschutz- und Informationssicherheitsziele Vertraulichkeit, Verfügbarkeit inkl. Belastbarkeit und Integrität auf www.datev.de/datenschutz zur Verfügung. Ferner veröffentlicht die DATEV eG das Whitepaper „Datenschutz und Unternehmenssicherheit bei DATEV".

3. Gesamtergebnis der Begutachtung

Die Begutachtung hat ergeben, dass die DATEV eG ein angemessenes, wirksames Informationssicherheits- und Datenschutzmanagementsystem nachhaltig umgesetzt hat und die Forderungen der Regelwerke ISO/IEC 27001 und ISO/IEC 27701 erfüllt. Insbesondere hat die Begutachtung ergeben, dass im Rahmen des Risikomanagements neben den Informationssicherheitsrisiken die Risiken für die Rechte und Freiheiten natürlicher Personen hinreichend berücksichtigt werden und bei der DATEV eG sehr vielfältige, umfassende und komplexe Informationssicherheits- und Datenschutz-maßnahmen bestehen, die einen hohen Vorsorgestand und einen sicheren Datenverarbeitungsbetrieb gewährleisten.

Die DATEV eG überprüft laufend die technischen und organisatorischen Maßnahmen in Form von regelmäßigen internen Prüfungen und Audits auf ihre Angemessenheit und Wirksamkeit und leitet daraus Korrektur- und Vorbeugungsmaßnahmen ab, die zur kontinuierlichen Verbesserung des Systems als Ganzes beitragen.

Hohe Synergien für den wirksamen Nachweis und die Kontrolle der technischen und organisatorischen Maßnahmen ergeben sich darüber hinaus durch die erfolgreiche Begutachtung nach ISO 9001 Qualitätsmanagement und ISO/IEC 20000-1 Service-management für den Bereich des Digital & Print Solution Centers sowie für die Entsorgung besonders sensibler Daten gemäß ISO 21964/DIN 66399-1. Damit können Mitglieder und Kunden zur Erfüllung Ihrer Prüfpflicht (Art. 28 und 32 DS-GVO) auf das vorliegende Informationssicherheits- und Datenschutzzertifikat auf www.datev.de/datenschutz zurückgreifen.

Bei der Begutachtung von Managementsystemen handelt es sich um eine stichproben-artige Überprüfung der Forderungen des Regelwerkes hinsichtlich der Umsetzung und dessen Dokumentation. Auf der Basis des Audits und der darin erbrachten Nachweise ist davon auszugehen, dass das Managementsystem die Anforderungen zum Auditzeitpunkt erfüllt. Die CIS übernimmt jedoch keine Gewähr oder Haftung für eine vollständige und dauerhafte Erfüllung des Regelwerkes während der Laufzeit der Bescheinigung, da dies alleinig in der Verantwortung des Unternehmens liegt.

Wien, 31. Dezember 2024

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Vienna, Salztorgasse 2/3/7

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com