UIMCommunic@tion
praxisnah.gut.informiert.

11/2022

Ausgabe für Deutschland

Inhaltsverzeichnis ++ ISO 27001:2022 ++ Abmahnwelle wegen Google Fonts ++ Jubiläumsrabatt für das eCollege ++ **Reminder:** Frist für die Umstellung der Standardvertragsklauseln läuft ab ++ **Inhaltsverzeichnis**

ISO 27001-Update: Was ändert sich? Was muss beachtet werden?

Zertifizierungen laufen aus; frühzeitiges Handeln empfehlenswert

Im Oktober 2022 wurde eine neue Version der ISO/IEC 27001 veröffentlicht. Der De-Facto-Standard der Informationssicherheit erfährt damit ein markantes Update in unsicheren Cyberzeiten. So formuliert die neue ISO-Version klare Anforderungen an ein Informationssicherheits-Managementsystem (ISMS). Dabei liegt der Nutzen von Zertifizierungen in Verbindung mit ISO-Normen in einer globalen Welt auf der Hand: „Eine Zertifizierung setzt Qualität voraus. Sie ist Ausdruck von Kompetenz und sorgt für Vertrauen. Ein echtes Qualitätssiegel," erklärt der Zertifizierungsexperte Dr. Jörn Voßbein anlässlich der ISO-Veröffentlichung. Für die Durchführung der Umstellung auf die neue Norm hat das International Accreditation Forum (IAF) die damit verbundenen Anforderungen für Akkreditierungsstellen, Zertifizierungsstellen und die zu prüfenden Organisationen ebenfalls veröffentlicht (IAF MD 26:2022). Zu beachten sind dabei, abgesehen von der aktualisierten Struktur, auch die elf neu aufgenommenen Maßnahmen, sowie vor allem der notwendige Handlungsbedarf für die Unternehmen, um die Umstellung erfolgreich zu meistern.

Zunächst ein Blick in die überarbeitete Struktur des Annex A: Die bisherige Themengliederung wurde aufgelöst. Die Maßnahmen werden zukünftig den vier Abschnitten „Organisatorische Maßnahmen" (37 Maßnahmen), „Personenbezogene Maßnahmen" (8 Maßnahmen), „Physische Maßnahmen" (14 Maßnahmen) und „Technologische Maßnahmen" (34 Maßnahmen) zugeordnet.

Elf neue Maßnahmen sind hinzugekommen. Drei zentrale Maßnahmen sind Datenmaskierung, Überwachung von Aktivitäten sowie Informationssicherheit für die Nutzung von Cloud-Diensten. Bei der „Datenmaskierung" sollen Daten so verändert werden, dass sie für einen Cyberkriminellen keinen oder nur geringen Nutzen haben. Bei der „Überwachung von Aktivitäten" geht es um die Überwachung der Unternehmens-IT, um dadurch ungewöhnliches Verhalten früh- und auch rechtzeitig erkennen zu können. Um die Nutzung von Cloud-Lösungen sicherer zu machen, sollen Unternehmen entsprechende Prozesse und Vorkehrungen entwickeln – besagt die Maßnahme „Informationssicherheit für die Nutzung von Cloud-Diensten".

Was gilt es nun von bereits zertifizierten Unternehmen zu beachten? Deadline für die Umstellung ist Oktober 2025. Im Herbst 2025 müssen alle alten ISO/IEC 27001:2013 bzw. ISO/IEC 27001:2017-Zertifikate zurückgezogen werden. Eine Umstellung sollte in jedem Fall vorher erfolgen. Das Audit muss dabei zwingend aus einem Vor-Ort-Audit bestehen und beinhaltet die Inaugenscheinnahme verschiedener Prüfungsfelder.

Wie lange bleibt Zeit? Unternehmen, die nach ISO/IEC 27001:2013 bzw. ISO/IEC 27001:2017 zertifiziert sind, haben nun drei Jahre Zeit, die Neuerungen umzusetzen.

„Das ISO 27001-Zertifikat ist kein Selbstzweck, sondern steigert die Cyber- und Informationssicherheit im eigenen Unternehmen. Die neue Norm ist eine gute Gelegenheit die internen Prozesse zu prüfen und wo notwendig zu aktualisieren", weist der erfahrene Informationssicherheitsexperte Dr. Jörn Voßbein auf die Bedeutung der Maßnahme hin.

Mehr Informationen unter www.uimc.de/news

Abmahnung bzgl. Google Fonts und kein Ende

Auch weiterhin „flattern" bei unseren Kunden viele Schadensersatzforderungen von dubiosen Anwaltskanzlein aufgrund der Nutzung von Google Fonts ein (siehe UIMCommunication 08/2022). Zum Teil stimmen die Vorwürfe nicht (mehr), zum Teil weisen die Schreiben gravierende Fehler auf. Grundsätzlich ist hierbei also unsere dringende Empfehlung nicht zu zahlen, sondern sich mit Ihrem Datenschutzbeauftragten abzustimmen.

UIMC Dr. Voßbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal
Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Wir freuen uns über Ihren Anruf!
+49 202 946 7726 200

UIMCommunication
praxisnah.gut.informiert.

Jubiläumsrabatt für eCollege nur noch bis zum 31.12.2022

Die UIMC feiert ihr 25-jähriges Jubiläum. Da auch Sie durch Ihre Treue zu unserem Erfolg beigetragen haben, erhalten Sie einen Rabatt von 25 % auf unsere E-Learning-Plattform, wenn Sie das „eCollege“ bis zum 31.12.2022 beauftragen.

Folgende Funktionen erhalten Sie:

- praxisbezogene Sensibilisierung und Wissensvermittlung
- **Selbst-Test** für Mitarbeiter (fördert Motivation und verbessert Wissensvermittlung)
- **elektronische Bestätigung** der umgesetzten Schulungen (kein Medienbruch durch Ausdruck eines PDF)
- Übersicht über absolvierte Schulungen für Personalabteilung (**Rechenschaftspflicht**)
- Erstellung eines **Zertifikats** für User
- Basis-Customizing an Ihr Unternehmen

Unter www.uimc.de/ecollege können Sie sowohl ein Produktvideo einsehen als auch problemlos einen unverbindlichen Demo-Account beantragen.

Warum E-Learning? Die Erfahrung zeigt, dass Vorgaben nur eingehalten werden, wenn Mitarbeiter die Hintergründe verstehen. Andernfalls werden entweder bewusst Regeln umgangen, weil sie als „lästig“ empfunden werden, oder es wird unbewusst aus Unwissen gegen diese verstoßen. So zeigt sich, dass viele Vorfälle durch nicht sensibilisierte oder unzureichend unterrichtete Mitarbeiter entstehen: Durch den sog. „unfreiwilligen Innentäter“. So stellte beispielsweise die letzte KES-Studie fest, dass die Verbesserung der Informationssicherheit maßgeblich durch das mangelnde Bewusstsein der Mitarbeiter behindert wird (über 70%; Rang 1). Die gesamte KES-Studie können Sie unter www.uimc.de/kes abrufen.

Zur effektiven Umsetzung von Anforderungen ist es unerlässlich, die Mitarbeiter zu sensibilisieren und auf die zu ergreifenden Maßnahmen zu schulen. Unser eCollege ist eine webbasierte Schulungsplattform, die über das Internet ohne Aufbau eigener Infrastruktur erreichbar ist. Hiermit können Mitarbeiter im Datenschutz und in der Informationssicherheit sensibilisiert und geschult werden. Unabhängig, ob Sie im Büro, im Home-Office oder unterwegs sind.

Reminder: Abschluss von Standardvertragsklauseln bis zum 27.12.2022

Seit Sommer 2021 gibt es neue Standardvertragsklauseln, die einen Datentransfer in Drittländer außerhalb der EU ermöglichen. Hintergrund war ein Urteil des EuGH, welches die alten Standards für unzulässig erklärt hat. Zur Umsetzung der neuen Verträge gab die EU-Kommission eine Übergangsfrist von 18 Monaten, die am 27. Dezember 2022 abläuft.

Die UIMC rät: Prüfen Sie, ob alle Standardverträge für den Drittlandtransfer auf dem aktuellen Stand sind.

Mehr Infos unter www.uimc.de/drittlandtransfer

Download der Verträge unter www.online-formular-center.eu (geschützter Bereich)

Aktuelles im Online-Formular-Center

Um über Neuerungen zeitnah informiert zu werden, können Sie unser News-Forum abonnieren und erhalten daraufhin eine E-Mail, sofern Sie einen personalisierten Account haben.

www.uimcollege.de

Mehr Informationen, Hinweise & Tipps finden Sie hier: https://www.UIMC.de/communication