IT insider

TECHNIK. BUSINESS. TRENDS.

So wird die Pflicht zur Kür

IT-INFRASTRUKTUR

Pflichtenheft für die IT
Hinsichtlich ihrer IT müssen Unternehmen einige Richtlinien und Vorgaben erfüllen. Ein Überblick.

IT-SUPPORT

DSGVO bleibt Dauerbaustelle
Neue Anforderungen sorgen dafür, dass sich die DSGVO in einem ständigen Prozess befindet.

IT-SICHERHEIT

NIS2 setzt neue Standards
Das Thema »NIS2-Richtlinie« beschäftigt – und fordert – viele Unternehmen. Jetzt aktiv werden!

IT-SERVICE .NETWORK

Sehr geehrte Damen und Herren, liebe Geschäftspartner,

wir leben in einer Zeit rasanter technologischer Entwicklungen, die ständig neue Möglichkeiten eröffnen, aber auch Herausforderungen und Verantwortlichkeiten mit sich bringen. In dieser Dynamik sind insbesondere die IT-Sicherheit und Compliance gefordert. Unternehmen aller Größen und Branchen werden dabei mit einem immer dichteren Geflecht aus Richtlinien und Standards konfrontiert – da fällt es manchmal schwer, den Wald vor lauter Bäumen zu sehen.

Und dieser Wald scheint ziemlich undurchdringlich zu sein: Vorschriften wie die DSGVO und die GoBD und neue Herausforderungen wie die NIS2-Richtlinie oder die Pflicht zur Zeiterfassung legen Unternehmen Barrieren in den Weg, die es zu überwinden gilt. Und sie verhindern, dass sich Betriebe auf das Wesentliche konzentrieren können – das Tagesgeschäft und die Weiterentwicklung des Unternehmens.

Die Richtlinien und Standards sind andererseits unerlässlich. Sie helfen, das Vertrauen in die digitale Infrastruktur zu stärken und die Sicherheit von Unternehmens- und Kundendaten zu gewährleisten. Ihre Komplexität und der rasche Wandel in der IT-Welt können dennoch überwältigend sein. Die Herausforderung liegt nicht nur im Verstehen und Implementieren dieser Richtlinien, sondern auch in der fortlaufenden Anpassung an neue Entwicklungen und Anforderungen.

In dieser Ausgabe unseres Kundenmagazins ITinsider greifen wir diese Thematik auf, wobei wir uns nicht in den Details der einzelnen Richtlinien verlieren wollen. Die Ausgabe soll einige der wichtigsten Vorgaben aufgreifen und zeigen, wie Unternehmen mit ihnen umgehen können – mit der Unterstützung von uns als ihrem IT-Dienstleister. Das übergeordnete Ziel sollte grundsätzlich sein, die richtige Balance zwischen Compliance, Sicherheit und betrieblicher Effizienz zu finden.

Lassen Sie uns gemeinsam diese Herausforderungen meistern und die Chancen nutzen, die sich daraus ergeben!

Wir wünschen Ihnen eine aufschlussreiche Lektüre!

Ihr Systemhaus

INHALT

IMPRESSUM

Herausgeber
SYNAXON AG | Falkenstraße 31 | D-33758 Schloß Holte-Stukenbrock
Telefon 05207 9299 – 200 | Fax 05207 9299 – 296
E-Mail info@synaxon.de | www.synaxon.de
Redaktion
André Vogtschmidt (V.i.S.d.P.), Janina Kröger
Ansprechpartner
André Vogtschmidt | andre.vogtschmidt@synaxon.de

Konzept/Gestaltung
Mirco Becker
Druck
Wentker Druck GmbH | Gutenbergstraße 5 – 7 | 48268 Greven
www.wentker-druck.de

Pflichten-heft für die IT

Je mehr die (Geschäfts-)Welt von IT-Systemen abhängt, desto wichtiger wird der Schutz dieser Systeme und der darin vorhandenen (Kunden-) Daten durch rechtliche Vorgaben und Richtlinien. Das Ergebnis dieser Entwicklung: Unternehmen jeder Größe sollten ein Pflichtenheft für die IT führen und umsetzen.

Richtlinien und Vorgaben: ein notwendiges Übel

Sowohl große Konzerne als auch kleine und mittelständische Unternehmen (KMU), Selbstständige und Kleinstunternehmen sind zunehmend von ihrer IT-Infrastruktur abhängig: Zahlreiche Prozesse und Geschäftsabläufe lassen sich in der digitalen Welt von heute nämlich nur noch mit Computer und Co. abbilden. Tatsächlich ist es auch so, dass die Digitalisierung zahlreiche Vorteile bietet – beispielsweise kann sie dabei helfen, betriebliche Abläufe zu automatisieren, manuellen Aufwand zu reduzieren und Geschäftsprozesse zu optimieren. Die zunehmende Abhängigkeit von Informationstechnologien bringt aber gleichzeitig signifikante Risiken mit sich, besonders in Bezug auf die Sicherheit von IT-Systemen und den Schutz sensibler Daten.

Genau deshalb gibt es inzwischen zahlreiche Vorgaben und Richtlinien, zu deren Umsetzung Unternehmen (teilweise) verpflichtet sind. Gesetze und Verordnungen wie die DSGVO, die GoBD oder die NIS2-Richtlinie sind unter anderem dazu gedacht, einen sicheren und verantwortungsvollen Umgang mit IT-Systemen und Unternehmensdaten zu fördern und die Resilienz gegenüber Cyberangriffen zu stärken. Indem sie Standards für Datenschutz, Datensicherheit und Compliance festlegen, sollen Richtlinien und Co. Unternehmen sowie ihre Kunden und Geschäftspartner absichern. Und aus diesem Grund ist ihre Existenz auch durchaus zu begrüßen. Das Problem: Die Komplexität und der Umfang rechtlicher Anforderungen können Unternehmen, die oft über begrenzte (IT-)Ressourcen verfügen, überwältigen.

IT-Pflichtenheft verschafft den Durchblick
Die Erstellung eines individuellen IT-Pflichtenhefts kann Unternehmen dabei helfen, die Vielzahl an rechtlichen Anforderungen, die je nach Unternehmensgröße und Branche variieren, zu verstehen und umzusetzen. Ein IT-Pflichtenheft sorgt dabei nicht nur dafür, einen Überblick über die erforderlichen Maßnahmen zu verschaffen; es bildet auch das Fundament dafür, dass diese Maßnahmen tatsächlich umgesetzt werden, um fortan einen sicheren, reibungslosen und gesetzeskonformen Betrieb der IT-Systeme zu gewährleisten.

Die Erstellung eines Pflichtenhefts für die IT und die Umsetzung der darin definierten Maßnahmen ist allerdings kein einmaliger Akt, sondern ein fortlaufender Prozess. Technologische Neuerungen und Änderungen in der Gesetzgebung erfordern eine regelmäßige Überprüfung und Anpassung der zur Einhaltung von Richtlinien und gesetzlichen Anforderungen durchgeführten Maßnahmen. Somit lässt sich ein IT-Pflichtenheft niemals als »erledigt« beiseite legen, sondern ist vielmehr eine unendliche Geschichte, die dafür sorgt, dass die IT-Infrastruktur dauerhaft nicht nur aktuell, sondern auch im Einklang mit allen relevanten Vorschriften bleibt.

Unwissenheit schützt vor Strafe nicht
Fakt ist: Die das individuelle Unternehmen betreffenden Richtlinien zu kennen und umzusetzen, ist kein Nice-to-have, sondern gehört schlicht zum Pflichtprogramm. Auch in diesem Zusammenhang greift nämlich der Grundsatz »Unwissenheit schützt vor Strafe nicht«. Verstöße gegen Datenschutzvorgaben oder Sicherheitsstandards können zu erheblichen Bußgeldern führen, die die finanzielle Stabilität eines Unternehmens gefährden können. Darüber hinaus kann die Nichteinhaltung solcher Vorschriften auch zu Reputationsverlusten führen, die nur schwer wieder gutzumachen sind.

Ein erfolgreich implementiertes IT-Pflichtenheft kann dabei nicht nur als Nachweis der Einhaltung gesetzlicher Vorgaben dienen, sondern auch als Instrument zur Steigerung der Effizienz und Sicherheit der IT-Systeme. Für Unternehmen, die diese Herausforderung meistern, können die Einhaltung rechtlicher Vorgaben und die Implementierung robuster IT-Sicherheitsstrategien zu einem Wettbewerbsvorteil werden. Indem sie Compliance als Chance begreifen, können KMU und Co. nicht nur rechtliche Risiken minimieren, sondern auch ihre Marktposition stärken und das Vertrauen ihrer Kunden festigen.

So wird die Pflicht zur Kür
Alle existierenden Richtlinien, Gesetze und Standards abbilden zu wollen, würde ein sehr viel umfassenderes Magazin erfordern, als Sie es gerade in der Hand halten (oder digital auf dem Bildschirm sehen). Wir haben versucht, die für Selbstständige, Kleinstunternehmen sowie KMU wichtigsten Anforderungen herauszupicken und dadurch einen Eindruck davon zu vermitteln, welche Art von Vorgaben es überhaupt gibt. Zudem gehen wir auf konkrete Maßnahmen ein, mit denen Unternehmen rechtliche Vorgaben erfüllen können.

Und natürlich möchten wir Ihnen unsere Unterstützung anbieten: Als IT-Dienstleister gehört es zu unserem Job, IT-Richtlinien zu kennen, zu verstehen und umzusetzen. Auch hier gilt: Angesichts der zahlreichen Vorgaben ist vielleicht nicht jeder Bereich unser Steckenpferd; wir können aber auf ein kompetentes Netzwerk an Systemhäusern zurückgreifen und finden dadurch immer einen Weg, um auch Ihnen bei Ihren individuellen Anliegen zur Seite zu stehen!

DSGVO: Datenschutz bleibt Dauerbaustelle

Die europäische Datenschutz-Grundverordnung gilt zwar schon seit dem 25. Mai 2018, doch auch Jahre später besteht in vielen Unternehmen immer noch Handlungsbedarf. Das zeigt sich zum Beispiel darin, dass die Aufsichtsbehörden weiterhin fleißig Bußgelder verhängen.

Was ist die DSGVO?
Die Datenschutz-Grundverordnung (DSGVO) ist seit dem 25. Mai 2018 das zentrale Datenschutzgesetz der Europäischen Union. Sie zielt darauf ab, die personenbezogenen Daten der EU-Bürger zu schützen und diejenigen, die diese Daten verarbeiten, zu regulieren. Die DSGVO verleiht den Bürgern umfassende Rechte bezüglich ihrer Daten – darunter das Recht auf Zugang, Berichtigung und Löschung ihrer Daten. Unternehmen und Organisationen, die personenbezogene Daten verarbeiten, müssen strenge Richtlinien zur Datensicherheit befolgen, ein hohes Maß an Transparenz gewährleisten und vor einer Datenverarbeitung grundsätzlich die Zustimmung der Nutzer einholen.

Weltweit hat die DSGVO einen neuen Standard für den Datenschutz gesetzt. Die Verordnung betrifft jedes Unternehmen, das personenbezogene Daten von EU-Bürgern verarbeitet, unabhängig davon, ob der Firmensitz in der EU liegt oder nicht. Das führt bis heute zu Querelen, vor allem weil der Datenverkehr zwischen der EU und Drittstaaten trotz mehrerer Anläufe für eine Regelung weiterhin problematisch ist.

DSGVO bleibt »Work in progress«
Seit ihrer Einführung hat die DSGVO kontinuierliche Anpassungen und Aktualisierungen erfahren, um mit den sich schnell ändernden Technologien und Datenschutzherausforderungen Schritt zu halten. In den Jahren 2023 und 2024 lag und liegt der Fokus verstärkt auf der Durchsetzung der Verordnung, der Schärfung der Richtlinien für internationale Datentransfers und der Anpassung an neue Technologien wie Künstliche Intelligenz und Big Data. Besonders bezüglich der KI-Nutzung sind datenschutzrechtlich aktuell noch viele Fragen offen. Es geht beispielsweise darum, sicherzustellen, dass KI-Systeme datenschutzkonforme Verfahren einhalten, insbesondere im Hinblick auf die Grundsätze der Datensparsamkeit und Zweckbindung. Auch die Frage, inwiefern Nutzer personenbezogene Daten, die von KI-Systemen verarbeitet werden, kontrollieren können, beschäftigt die Datenschützer ganz besonders. Sicher ist, dass es ihnen angesichts der raschen Entwicklungen in diesem Bereich so schnell nicht langweilig werden wird.

Offene Baustellen auch in Unternehmen
Aber nicht nur für Datenschützer bleibt die DSGVO aus den genannten – und weiteren – Gründen ein »Work in progress«; auch Unternehmen sind gefordert, ihre Datenschutzpraktiken kontinuierlich zu überprüfen und zu aktualisieren, um Konformität zu gewährleisten. Nach wie vor gibt es bei einigen Unternehmen deutlichen Nachholbedarf. Das zeigt sich darin, dass die zuständigen Aufsichtsbehörden weiterhin auf Datenschutzmängel stoßen und sich gezwungen sehen, Bußgelder zu verhängen.

Häufige Datenpannen waren in den vergangenen Jahren z.B. der Fehlversand und der Verlust von postalischen Unterlagen, offene E-Mail-Verteiler (mit den Adressen der Empänger im für alle einsehbaren CC-Bereich statt im verborgenen BCC-Bereich), das Abhandenkommen von Datenträgern durch Einbruch oder Diebstahl und das Abgreifen personenbezogener Daten durch Cyberkriminalität. Zudem verhängten deutsche Aufsichtsbehörden Sanktionen wegen unzulässiger Videoüberwachung.

IT-Sicherheit haucht DSGVO Leben ein
Fakt ist: Die Einhaltung der DSGVO ist keine Option, sondern eine absolute Notwendigkeit für Unternehmen, Einrichtungen und Organisationen jeder Größe, die mit personenbezogenen Daten (von EU-Bürgern) arbeiten. Gefordert ist hier die IT-Sicherheit: Sie ist nämlich dafür verantwortlich, jene Standards und Regeln, die die DSGVO für den Datenschutz festlegt, mit den dafür notwendigen technischen und organisatorischen Maßnahmen zu erfüllen und zu erhalten. Und das kann durchaus kompliziert sein.

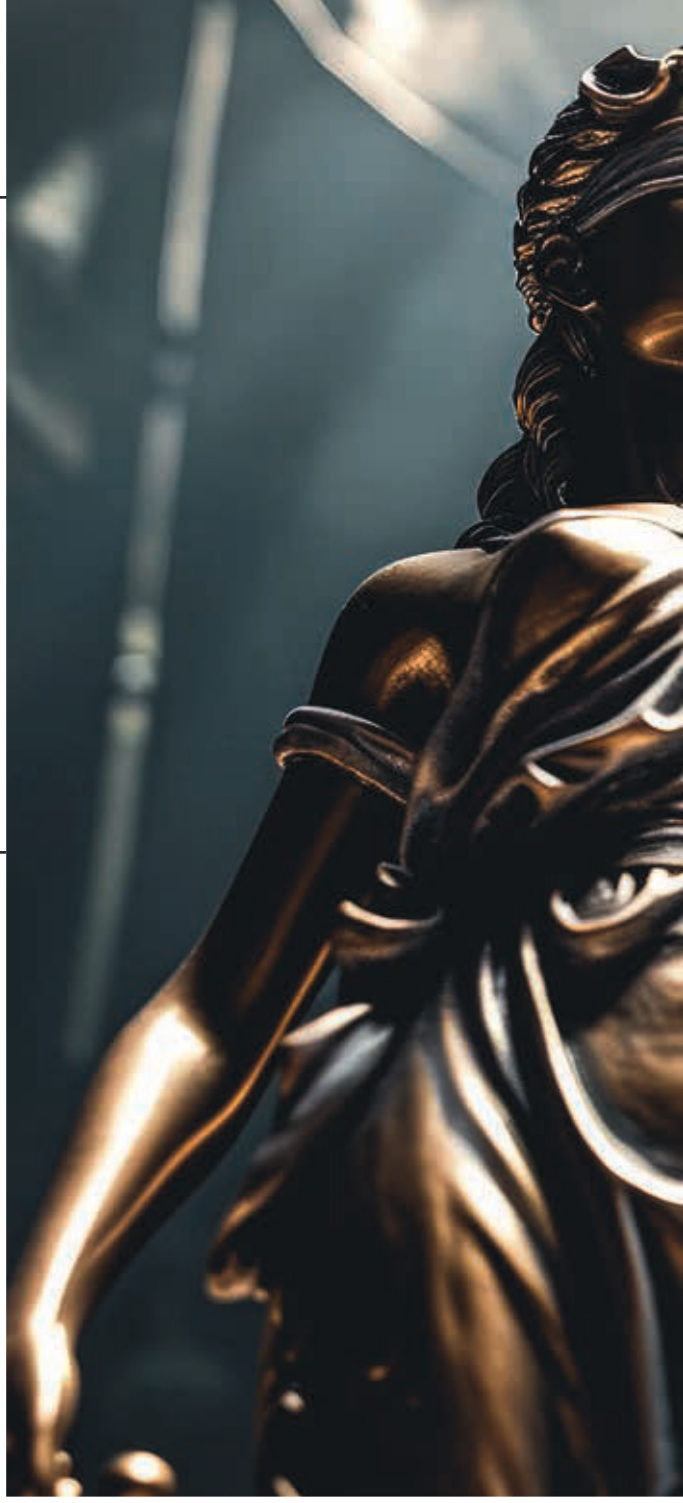
Als wäre dies nicht Herausforderung genug, soll die überarbeitete ePrivacy-Verordnung die DSGVO zukünftig ergänzen. Während die DSGVO den allgemeinen Rahmen für den Datenschutz bietet und alle Arten der Verarbeitung personenbezogener Daten abdeckt, zielt die ePrivacy-Verordnung speziell auf die Privatsphäre in der elektronischen Kommunikation ab. Zu den Kernpunkten gehören die Erweiterung des Rechts auf Vergessenwerden, ein Verbot der Direktwerbung ohne Zustimmung und strengere Cookie-Anforderungen.

Unsicherheiten beim Datenschutz?
Besonders für Selbstständige, Kleinstunternehmen und KMU mag die DSGVO sehr komplex erscheinen. Unser Tipp: Sehen Sie die DSGVO nicht als bloße rechtliche Hürde, sondern als Chance, das Vertrauen von Kunden und Geschäftspartnern zu stärken. Die Investition in Datenschutz ist eine Investition in die Zukunft Ihres Unternehmens und die Sicherheit Ihrer Kunden. Wir unterstützen Sie gern bei der Umsetzung!

DSGVO: die wichtigsten Aufgaben

- Integrieren Sie Datenschutz durch Technik und Voreinstellungen in Ihre Produkte und Dienstleistungen, indem Sie Daten standardmäßig schützen und nur absolut notwendige Daten erheben.
- Informieren Sie klar und verständlich über die Erhebung, Verwendung und Speicherung von Daten – am besten durch eine präzise Datenschutzerklärung.
- Holen Sie bei betroffenen Personen eine klare, informierte und freiwillige Zustimmung für datenbasierte Dienste ein, die jederzeit widerrufbar sein muss.
- Führen Sie für Verarbeitungstätigkeiten eine Datenschutz-Folgenabschätzung durch, wenn ein hohes Risiko für Rechte und Freiheiten von Personen besteht.
- Melden Sie Datenschutzverletzungen innerhalb von 72 Stunden an die zuständigen Behörden und informieren Sie betroffene Personen bei hohem Risiko.
- Stellen Sie sicher, dass betroffene Personen ihre Rechte ausüben können – darunter Auskunft, Berichtigung, Löschung und Widerspruch gegen die Verarbeitung.
- Führen Sie ein Verzeichnis aller Datenverarbeitungsaktivitäten, die personenbezogene Daten betreffen, um Ihre Konformität mit der DSGVO zu demonstrieren.
- Bestellen Sie einen Datenschutzbeauftragten, falls Ihre Kerntätigkeit in der umfangreichen Verarbeitung besonderer Datenkategorien besteht.

GoBD – rechtlich abgesichert



Hätten Sie gedacht, dass Sie vor Gericht landen könnten, weil Sie E-Mails nicht richtig archiviert haben? Unternehmen, die bei einer Betriebsprüfung keine gesetzeskonforme E-Mail-Archivierung vorweisen können, müssen mit harten Konsequenzen rechnen: Es drohen Strafzahlungen in nicht unerheblicher Höhe!

Betriebsprüfer kennen kein Pardon

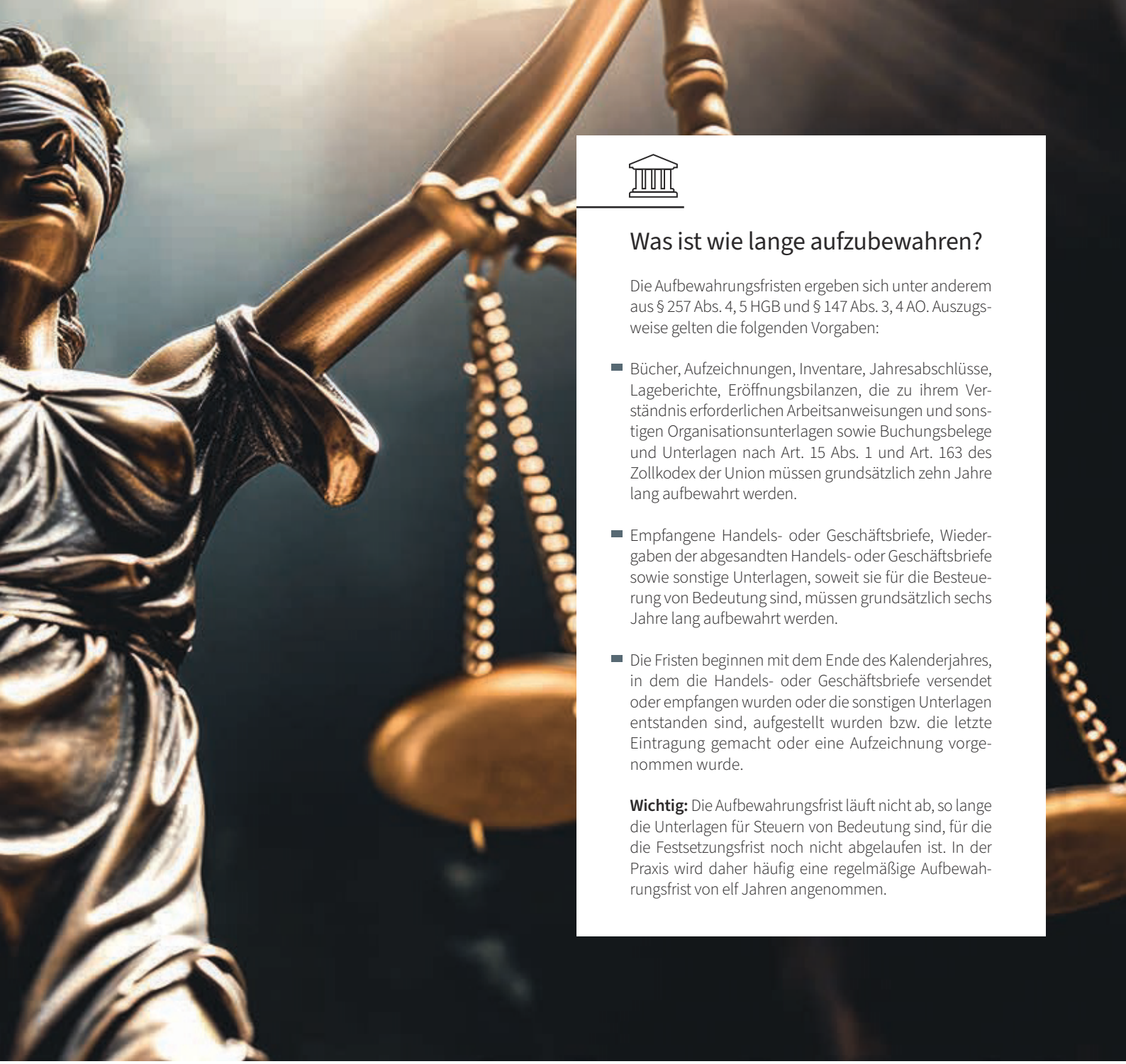
In einem konkreten Fall, der hier anonymisiert als Beispiel dienen soll, hat es ein Unternehmen aus dem Bereich KMU getroffen. Im Zuge einer Betriebsprüfung stellte sich heraus, dass das Unternehmen keine E-Mail-Archivierung vorweisen konnte. Trotz der Empfehlung seines IT-Dienstleisters hatte das Unternehmen darauf verzichtet. Warum? Weil eine E-Mail-Archivierung nach Aussage des Steuerberaters nicht notwendig sei. Pustekuchen. Ein Kostenbescheid flatterte ins Unternehmen, verlangt wurde eine Strafzahlung in Höhe von vier Prozent des Jahresumsatzes – ein sechsstelliger Betrag! Und weil der IT-Dienstleister per Gesprächsprotokoll vorweisen konnte, dass er auf die Pflicht zur E-Mail-Archivierung hingewiesen hatte, konnte das betroffene Unternehmen weder dem Dienstleister noch dem Steuerberater den schwarzen Peter zuschieben – was es über einen Gerichtsprozess versuchte.

Dieser Fall zeigt: Wenn es um eine fehlende E-Mail-Archivierung geht, kennen Betriebsprüfer kein Pardon. Im Gegenteil: Sie sind scheinbar gezielt hinter Unternehmen her, die auf die Archivierung verzichten und sich damit nicht an die gesetzlichen Vorgaben halten. Diese manifestieren sich in den GoBD. Die Abkürzung steht für die »Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff« – und ist damit eindeutig der Kategorie »Wie sperrig wollen wir eine Gesetzgebung formulieren?« zuzuordnen. Aber ob sperrig oder nicht: Fakt ist, dass Unternehmen die GoBD einhalten müssen.

GoBD – was ist das?

In Zeiten, in denen ein Großteil der Geschäftskommunikation per E-Mail abläuft und auch die Buchführung in elektronischer Form stattfindet, sollen die GoBD sicherstellen, dass die Buchführung mit allen relevanten Dokumenten und Informationen sauber, sicher und jederzeit nachprüfbar ist. Kurzum: Unternehmen müssen dafür sorgen, dass Betriebsprüfer bei einem Besuch direkt den Durchblick haben. Und das geht nur, wenn per E-Mail eingegangene, steuerrechtlich relevante Schriftstücke nach ihrer Bearbeitung nicht im Papierkorb landen, sondern nachvollziehbar, vollständig, richtig, zeitgerecht, geordnet und unverfälscht abgebildet und aufbewahrt werden.

Die Archivierung von E-Mails und anderen elektronischen Dokumenten gewährleistet also, dass Unternehmen eine lückenlose Historie aller geschäftlichen Transaktionen führen. Und dies ist sowohl für die Finanzverwaltung wichtig, als auch ein wertvolles Instrument für die interne Überprüfung und Analyse von Geschäftsprozessen.



Was ist wie lange aufzubewahren?

Die Aufbewahrungsfristen ergeben sich unter anderem aus § 257 Abs. 4, 5 HGB und § 147 Abs. 3, 4 AO. Auszugsweise gelten die folgenden Vorgaben:

- Bücher, Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen, die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen sowie Buchungsbelege und Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union müssen grundsätzlich zehn Jahre lang aufbewahrt werden.

- Empfangene Handels- oder Geschäftsbriefe, Wiedergaben der abgesandten Handels- oder Geschäftsbriefe sowie sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind, müssen grundsätzlich sechs Jahre lang aufbewahrt werden.

- Die Fristen beginnen mit dem Ende des Kalenderjahres, in dem die Handels- oder Geschäftsbriefe versendet oder empfangen wurden oder die sonstigen Unterlagen entstanden sind, aufgestellt wurden bzw. die letzte Eintragung gemacht oder eine Aufzeichnung vorgenommen wurde.

Wichtig: Die Aufbewahrungsfrist läuft nicht ab, so lange die Unterlagen für Steuern von Bedeutung sind, für die die Festsetzungsfrist noch nicht abgelaufen ist. In der Praxis wird daher häufig eine regelmäßige Aufbewahrungsfrist von elf Jahren angenommen.

Tool zur E-Mail-Archivierung sichert KMU ab

Die Umsetzung der GoBD ist eigentlich ganz einfach: Ein professionelles Tool zur E-Mail-Archivierung nimmt nicht nur die Sorge vor einer Betriebsprüfung, sondern stellt auch sicher, dass die elektronische Kommunikation den GoBD entspricht. Diese Tools arbeiten automatisch im Hintergrund und archivieren jede ein- und ausgehende E-Mail nach den Vorgaben der GoBD. Dadurch sind dann alle E-Mails vollständig, unveränderbar und jederzeit auffindbar gespeichert – und Unternehmen können im Handumdrehen nachweisen, dass ihre E-Mail-Archivierung die gesetzlichen Anforderungen erfüllt.

Darüber hinaus bieten diese Systeme weitere Vorteile: Sie verbessern die Effizienz bei der Suche und Verwaltung von E-Mails und helfen dabei, die Sicherheit der elektronischen Kommunikation zu erhöhen. Ob es um den Schutz vor Datenverlust, um Compliance-Anforderungen oder einfach um die Optimierung der Geschäftsprozesse geht – ein E-Mail-Archivierungssystem ist die Investition wert.

Die GoBD ernst nehmen – ein Muss für jedes Unternehmen

Die Umsetzung der GoBD ist ein Muss für jedes Unternehmen. Der zuvor beschriebene Fall ist nur ein Beispiel von vielen, in denen Betriebe Strafzahlungen leisten mussten, weil sie die Bedeutung der GoBD unterschätzt hatten. Um solche Szenarien zu vermeiden, sollten Sie die richtigen Maßnahmen ergreifen und in ein System investieren, das nicht nur die Compliance sicherstellt, sondern auch die Effizienz und Sicherheit der Unternehmenskommunikation verbessert.

Als IT-Dienstleister haben wir dafür natürlich die passenden Tools zur Hand – zum Beispiel die Managed E-Mail-Archivierung von SYNAXON SERVICES. Einmal installiert und eingerichtet, sorgt diese Lösung für eine unveränderbare und revisionssichere Ablage Ihrer E-Mails. Dank komplexer Verschlüsselungsverfahren ist eine hohe Datensicherheit gewährleistet. Die Datenablage erfolgt sicher auf deutschen Servern und ist über einen webbasierten Zugriff jederzeit erreichbar. Sie möchten mehr erfahren? Dann sprechen Sie uns gern an!

Gesetz trifft Praxis: Arbeitszeiten erfassen

Im Mai 2019 hat der Europäische Gerichtshof (EuGH) die Erfassung der Arbeitszeit zur Pflicht erklärt. Das Bundesarbeitsgericht (BAG) hat im September 2022 nachgezogen und das Urteil des EuGH bestätigt. Das bedeutet für Unternehmen: Ein Zeiterfassungssystem muss her!

EuGH-Urteil: Zeiterfassung ist ein Muss

Der Europäische Gerichtshof (EuGH) hat den Ball ins Rollen gebracht: Am 14. Mai 2019 verhandelte er eine Rechtssache, in der die spanische Gewerkschaft CCOO gegen eine Niederlassung der Deutschen Bank in Spanien Klage erhoben hatte. Im Kern ging es um die Frage, ob Arbeitszeiten generell oder lediglich die geleisteten Überstunden zu erfassen sind. Das Ergebnis der Verhandlung war ein Urteil, in dem der EuGH die »Verpflichtung zur Einrichtung eines Systems, mit dem die von einem jeden Arbeitnehmer geleistete tägliche Arbeitszeit gemessen werden kann,« beschlossen hat.

Die Intention dahinter ist durchaus zu unterstützen: Es geht nämlich darum, die Rechte der Arbeitnehmer zu stärken und ihre Gesundheit zu schützen. Die Pflicht zur Arbeitszeiterfassung ist dabei ein entscheidender Schritt: Die Dokumentation der Arbeitszeit soll verhindern, dass Arbeitnehmer durch endlose Überstunden ausbrennen und krank werden – und damit soll die gesetzliche Verpflichtung der Zeiterfassung die Arbeitsbedingungen verbessern.

EU-Mitgliedsstaaten sind gefordert

Danach lag der Ball dann bei den EU-Mitgliedsstaaten: Sie wurden aufgefordert, die notwendigen nationalen Gesetze zu erlassen, mit denen sie Arbeitgeber gemäß dem EuGH-Urteil zur Arbeitszeiterfassung verpflichten. Es hat in einigen Ländern allerdings teilweise recht lange gedauert, bis sie den Ball tatsächlich aufgenommen haben. Zum Beispiel in Deutschland. Hier ist der Ball auch 2024, also fünf Jahre später, immer noch nicht im Tor versenkt – aber immerhin geht es inzwischen in diese Richtung.

Denn: Mit Beschluss vom 13. September 2022 hat das Bundesarbeitsgericht (BAG) ebenfalls festgesetzt, dass in Deutschland die gesamte Arbeitszeit der Arbeitnehmer aufzuzeichnen ist, und damit das EuGH-Urteil bestätigt. Nach § 3 Abs. 2 Nr. 1 des Arbeitsschutzgesetzes (ArbSchG) sind Arbeitgeber nun also verpflichtet, ein System einzuführen, mit dem die geleistete Arbeitszeit erfasst werden kann. Offen ist allerdings noch, wie die Umsetzung eines solchen Systems konkret aussehen soll.

Aufzeichnungspflicht – aber wie?

Um die Frage des »Wie« der Aufzeichnungspflicht zu klären, ist das Bundesministerium für Arbeit und Soziales (BMAS) jetzt am Zug. Schon im April 2023 ist ein Vorschlag zur Ausgestaltung der Arbeitszeiterfassung im Arbeitszeitgesetz sowie im Jugendarbeitsschutzgesetz erstellt worden. Laut dem BMAS wird dieser Vorschlag derzeit regierungsintern beraten. 2024 könnte nun endlich Rechtsklarheit geschaffen werden. Für Arbeitgeber wichtig:

Unabhängig davon gilt die Pflicht zur Arbeitszeiterfassung aber schon längst.

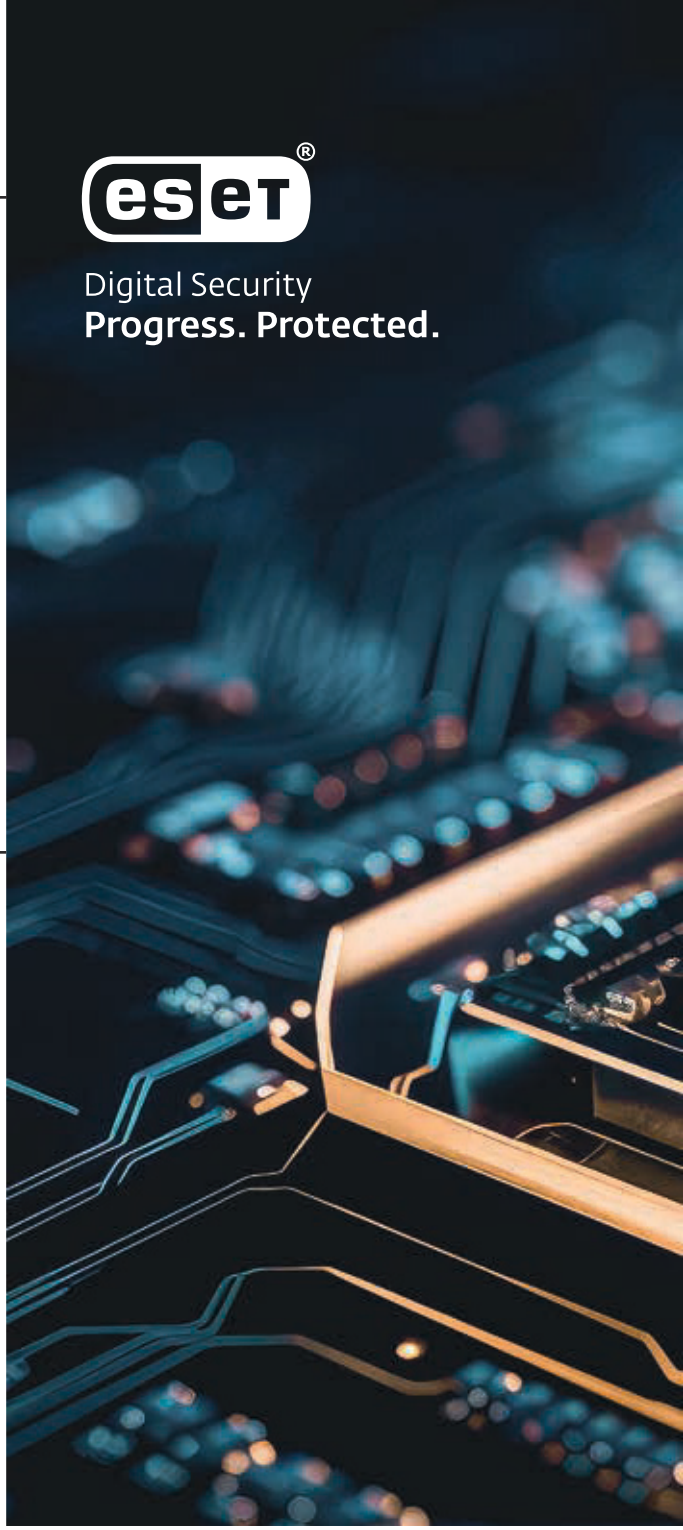
Das ist spätestens seit Februar 2020 klar, als sich das Emdener Arbeitsgericht bereits auf das EuGH-Urteil berufen hat. Ein Bauhelfer klagte gegen seinen früheren Arbeitgeber wegen Differenzen zwischen seinen privaten Arbeitszeitaufzeichnungen und den im Bautagebuch vermerkten Zeiten, die zur Lohnabrechnung herangezogen worden waren – zu seinem Nachteil. Er verlangte eine Nachzahlung und bekam Recht: Das Gericht bestätigte, dass ein Bautagebuch, das individuelle Arbeits-, Fahrt- und Rüstzeiten nicht adäquat erfasst, für die Arbeitszeiterfassung nicht geeignet ist.

Zeiten richtig dokumentieren

Für viele Unternehmen stellt sich aber weiterhin die Frage, wie eine objektive und zuverlässige Erfassung der täglichen Arbeitszeit, wie der EuGH sie fordert, möglich ist. Gut zu wissen: Da der EuGH keine konkreten Angaben zur Umsetzung der Aufzeichnungspflicht macht, haben Unternehmen bei der Entscheidung für eine Methode freie Wahl. Prinzipiell würden schon ein per Hand ausgefüllter Stundenzettel oder auch eine Excel-Tabelle ausreichen. Zu empfehlen sind diese Methoden allerdings nicht, denn sie sind für Fehler oder Manipulation anfällig und zudem zeitintensiv.

Daher rücken digitale Zeiterfassungssysteme in den Fokus. Diese Systeme bieten eine Vielzahl von Vorteilen gegenüber herkömmlichen Methoden wie einem schnöden Stundenzettel auf Papier. Digitale Lösungen ermöglichen eine präzise und unkomplizierte Erfassung der Arbeitszeit – sowohl für Remote-Arbeit als auch für traditionelle Arbeitsumgebungen. Sie bieten unter anderem Funktionen wie die Echtzeit-Überwachung, automatische Pausenerkennung und eine projekt- oder kundenspezifische Zuordnung. Achtung: Auch bei digitalen Lösungen ist darauf zu achten, dass eine Manipulation nicht möglich ist.

Die Implementierung digitaler Systeme kann die Einhaltung gesetzlicher Vorschriften und die interne Prozesseffizienz auf jeden Fall unterstützen. Durch die Automatisierung der Zeiterfassung können Unternehmen administrative Aufwände reduzieren und eine transparente Grundlage für die Lohnabrechnung schaffen. Hört sich gut an? Dann nehmen Sie Kontakt zu uns auf und lassen Sie sich von uns zu diesem Thema beraten!



NIS2 setzt neue Standards

Im Jahr 2024 ist sie das Thema Nr. 1: die sogenannte NIS2-Richtlinie. Die EU will mit der überarbeiteten Richtlinie zur Sicherheit von Netz- und Informationssystemen die Resilienz bzw. Cybersicherheit verbessern. Zahlreiche Unternehmen werden durch die EU-weit geltenden Standards in die Pflicht genommen.

Cybercrime weiterhin auf Rekordniveau

Jedes Jahr aufs Neue warnt das BSI mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland vor einem Cybercrime-Geschehen auf Rekordniveau. Fakt ist: Cyberkriminelle geben keine Ruhe – und das bedeutet für die potenziellen Opfer, dass sie jederzeit gegenüber Angriffsversuchen wachsam sein sollten. In vielen Einrichtungen und Unternehmen ist die IT-Infrastruktur aber weiterhin nicht angemessen geschützt. Genau das soll die NIS2-Richtlinie europaweit ändern.

Was ist die NIS2-Richtlinie?

Die NIS2-Richtlinie bezeichnet ein europäisches Regelwerk, das darauf abzielt, einheitliche Mindeststandards für die Cybersicherheit zu definieren und dadurch die Resilienz von Einrichtungen und Unternehmen zu verbessern – und damit auch die Widerstandsfähigkeit der gesamten EU. Während die Abkürzung NIS für »Network and Information Security« steht, verrät die Ziffer »2«, dass es sich um eine zweite Fassung der 2016 veröffentlichten NIS-Richtlinie handelt.

Die NIS2-Richtlinie ist am 16. Januar 2023 in Kraft getreten, ihre Umsetzung in nationales Recht ist bis zum 17. Oktober 2024 vorgesehen. Unternehmen, die die Vorgaben danach nicht einhalten, müssen mit Konsequenzen rechnen: Möglich ist, dass Geldstrafen verhängt werden; die Zertifizierung oder Erlaubnis für den Betrieb eines Geschäfts könnten zeitweilig widerrufen werden; leitende Angestellte könnten gemäß der nationalen Gesetze persönlich haftbar gemacht werden.

Kreis der betroffenen Unternehmen wird größer

Eine maßgebliche Neuerung bei NIS2 ist, dass deutlich mehr Unternehmen betroffen sind, als zuvor. Dabei werden zwei Bereiche abgesteckt. Bei den »wesentlichen Einrichtungen« handelt es sich um große Organisationen in Sektoren mit hoher Kritikalität aus den Bereichen Energie, Verkehr, Bankwesen, Verwaltung von IKT-Diensten, Trinkwasser, Abwasser, Gesundheitswesen, Digitale Infrastruktur, Öffentliche Verwaltung, Finanzmarktinfrastruktur und Weltraum. Unter »wichtige Einrichtungen« fallen große Organisationen sonstiger kritischer Sektoren und mittelständische Unternehmen – darunter Post- und Kurierdienste, die Abfallwirtschaft, Produktion, Herstellung/Handel mit chemischen Stoffen, Produktion, Verarbeitung/Vertrieb von Lebensmitteln, das verarbeitende Gewerbe/die Warenherstellung, Anbieter digitaler Dienste und die Forschung. Für die betroffenen mittelständischen und großen Betriebe gelten als Eckdaten: mittel – 50 bis 250 Beschäftigte sowie 10 bis 50 Mio. € Umsatz/Jahr und/oder eine jährliche Bilanzsumme von weniger als

Mit ESET die NIS2 erfüllen!

ESET, als einer der weltweit führenden Hersteller von IT-Security-Lösungen, hat sich intensiv mit der neuen NIS2-Richtlinie befasst und sichergestellt, dass die eigenen Produkte Unternehmen bei der Einhaltung der Vorgaben unterstützen. Mit dem Multi-Secured-Endpoint-Ansatz setzt ESET beispielsweise das Fundament für eine Zero Trust Security. Dafür kombiniert der Software-Hersteller Endpoint Protection, Verschlüsselung, Multi-Faktor-Authentifizierung, Schutz für Cloud-Anwendungen und das Cloud Sandboxing miteinander. Unternehmen können aus verschiedenen ESET PROTECT Bundles wählen und auf diese Weise eine maßgeschneiderte IT-Sicherheitsstrategie umsetzen. Gern beraten wir Sie zu den Möglichkeiten und erarbeiten gemeinsam mit Ihnen ein Konzept, das die Anforderungen der NIS2-Richtlinie erfüllt.

Zögern Sie nicht und sprechen Sie uns an!

43 Mio. €; groß – mehr als 250 Beschäftigte sowie mehr als 50 Mio. € Umsatz/Jahr und/oder eine jährliche Bilanzsumme von mehr als 43 Mio. €.

Welche Maßnahmen müssen umgesetzt werden?
Die NIS2-Richtlinie verlangt betroffenen Unternehmen einiges ab. Der Maßnahmenkatalog umfasst eine lange Liste sowohl technischer als auch organisatorischer Maßnahmen. Betroffene Unternehmen sind unter anderem verpflichtet, wirksame Risikoanalysen durchzuführen, Richtlinien für die (Cyber-)Sicherheit von Informationssystemen aufzustellen, ihre Lieferketten abzusichern und Krisen-Management-Pläne zur Aufrechterhaltung des Betriebs im Krisenfall zu erstellen.

Darüber hinaus sind Unternehmen und Einrichtungen aufgefordert, Praktiken zur Cyberhygiene anzuwenden. Dazu zählen Zero-Trust-Grundsätze, regelmäßige Software-Updates, sichere Gerätekonfigurationen, Netzwerksegmentierungen, ein Identitäts- und Zugriffsmanagement sowie die Sensibilisierung und Schulung der Mitarbeiter für Cyberbedrohungen wie Social-Engineering-Techniken. Nicht zuletzt gilt es, Sorgfalts- und Berichtspflichten zu erfüllen. Im Fall eines Sicherheitsvorfalls sind Unternehmen und Einrichtungen zum Beispiel verpflichtet, innerhalb von 24 Stunden eine erste Meldung abzusetzen und innerhalb von 72 Stunden Detailinformationen zu liefern.

Cybersicherheit fordert Unternehmen jeder Größe
Die Mehrheit der kleinen und mittelständischen Unternehmen fällt nicht unter die NIS2-Richtlinie. Aber: Ausnahmen bestätigen die Regel. Das kann beispielsweise dann der Fall sein, wenn KMU Teil der Lieferkette von Unternehmen sind, die die NIS2-Richtlinie einhalten müssen. Experten vermuten außerdem, dass KMU in der Lieferkette künftig verstärkt Ziel von Cyberattacken werden könnten, da sie vermeintlich weniger geschützt sind und Angriffe auf die gesamte Lieferkette ermöglichen.

Gefahr erkannt? Gefahr gebannt!

Cyberrisiken lauern überall und sind auch für kleine Unternehmen ein Problem. Sie müssen sicherstellen, dass ihre IT-Infrastruktur bestmöglich geschützt ist – und das mit manchmal wenigen personellen und finanziellen Ressourcen. Der Cyber-Risiko-Check soll jetzt dabei helfen.

Großes Thema für kleine Firmen
Cyberkriminelle fokussieren sich mit ihren Attacken längst nicht mehr ausschließlich auf große, zahlungskräftige Unternehmen; vielmehr sind zunehmend auch (Kleinst-)Unternehmen mit bis zu 50 Mitarbeitern das Ziel von Cyberangriffen. Umso wichtiger ist es daher, dass sich diese Zielgruppe für die zunehmenden Gefahren von Cyberangriffen wappnet und ihren Fokus verstärkt auf die Sicherheit ihrer Daten und Systeme richtet. Es gilt, geeignete Maßnahmen zu ergreifen, um sich vor potenziellen Bedrohungen zu schützen und den Geschäftsbetrieb abzusichern.

Aber wie lässt sich das Thema Cybersicherheit am besten stemmen – vor allem angesichts der begrenzten personellen, zeitlichen und finanziellen Ressourcen, die klein(st)en Unternehmen meist nur zur Verfügung stehen? Unser Tipp: Mit dem Cyber-Risiko-Check packen kleine Unternehmen dieses große Thema an!

Was ist der Cyber-Risiko-Check?
Der Cyber-Risiko-Check (auch: DIN SPEC 27076 »IT-Sicherheitsberatung für kleine und Kleinstunternehmen«) ist ein neuer Beratungsstandard, der von einem Konsortium unter der Leitung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und dem Bundesverband mittelständische Wirtschaft (BVMW) entwickelt worden ist. Er soll die IT- und Informationssicherheit kosten- und zeiteffizient verbessern und innerhalb kürzester Zeit gefährliche Schwachstellen aufdecken.

Dazu geht ein beauftragter IT-Dienstleister einen Fragebogen mit Anforderungen durch, die kleine Betriebe erfüllen müssen, um die relevantesten Risiken zu minimieren und Einfallstore für Angreifer zu schließen. Es geht hier um Maßnahmen, die kleine Betriebe mit wenigen Beschäftigten realistisch umsetzen können. Im Anschluss erhalten die Unternehmen einen Ergebnisbericht inklusive eines Risiko-Statuswerts und konkreten Handlungsempfehlungen. Damit macht der neue Standard den Sicherheitsstand von Unternehmen messbar.

Cyber-Risiko-Check – und dann?
Es hilft aber nicht, mit dem Ergebnisbericht die Handlungsempfehlungen nur auf Papier zu haben. Vielmehr sollten sich Unternehmen nach der Beratung daran machen, die Maßnahmen umzusetzen – am besten in Zusammenarbeit mit einem IT-Dienstleister. Ein weiterer Tipp: Nach der Umsetzung lohnt sich eine Wiederholung des Cyber-Risiko-Checks, um zu prüfen, ob sich der Statuswert tatsächlich verbessert hat.

Wichtig zu bedenken ist, dass der Cyber-Risiko-Check bewusst nur das absolute Minimum an Anforderungen an die IT-Sicherheit überprüft. Daher gewährleistet auch das das Erreichen des Maximalwerts keine vollumfängliche Sicherheit. Es handelt sich beim Cyber-Risiko-Check zudem nicht um eine IT-Sicherheitszertifizierung. Dennoch hilft er Unternehmen, das eigene IT-Sicherheitsniveau zu bewerten und sich durch konkrete Maßnahmen besser zu schützen.

Wir packen IT-Sicherheit mit Ihnen an!
Es gibt hinsichtlich der Absicherung gegen Cyberangriffe also noch Luft nach oben. Grundsätzlich gilt nämlich auch, dass die Umsetzung von IT-Sicherheit ein Prozess ist, der langfristig zu verfolgen ist. Denn: Aufgrund der sich stetig verändernden Bedrohungslage sind immer wieder Anpassungen notwendig. Wir helfen Unternehmen, am Ball zu bleiben und die IT-Landschaft so sicher wie möglich zu machen!

Cyber-Risiko-Check fördern lassen

Kleine Unternehmen können für die Beratung nach DIN SPEC 27076 Fördermittel erhalten. Zur Kofinanzierung stehen verschiedene Fördertöpfe bereit. Das Programm »go-digital« des Bundes beispielsweise fördert unter anderem Maßnahmen für eine »Digitalisierungsstrategie« und mehr »IT-Sicherheit«. Unternehmen erhalten dabei einen Zuschuss, der maximal 50 Prozent der Gesamtinvestition abdeckt. Das Programm läuft noch bis 2025, die Beantragung erfolgt über lizenzierte Berater. Bei der »Förderung von Unternehmensberatung für KMU« handelt es sich um ein neues Programm des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Hiermit lassen sich Beratungsleistungen zur Digitalisierung bezuschussen. Das Programm läuft bis 2026, die Beantragung erfolgt über die BAFA. Auch die Bundesländer bieten verschiedene Förderprogramme an.

So läuft der Cyber-Risiko-Check ab

Damit der Aufwand bei den Unternehmen so gering wie möglich ist, wird der Cyber-Risiko-Check durch spezialisierte IT-Dienstleister wie folgt durchgeführt:

- Informatives Erstgespräch: Unternehmen werden über den Ablauf und benötigte Dokumente (z. B. Backup-Konzepte, Sicherheitsrichtlinien, Vertraulichkeitserklärungen, Notfallpläne) informiert. Erste Unternehmensdaten werden aufgenommen.
- Aufnahme des Ist-Zustands: Bei diesem Termin (online, offline oder hybrid) geht der IT-Dienstleister mit der Geschäftsführung und dem/den IT-Verantwortlichen in bis zu drei Stunden den Fragebogen durch und dokumentiert die Antworten.
- Auswertung und Berichterstellung: Es folgen die Auswertung der erhobenen Daten, die Errechnung des Risiko-Statuswerts und die Erstellung eines Berichts.
- Ergebnispräsentation: Der IT-Dienstleister stellt den Bericht vor, geht auf (un)erfüllte Anforderungen ein und gibt Handlungsempfehlungen mit Priorisierung.

Damit sich Mut nicht rächt

Edward Snowden ist ein Beispiel dafür, dass es sich rächen kann, Missstände aufdecken zu wollen. Das deutsche Hinweisgeberschutzgesetz soll solche Fälle verhindern. Es verpflichtet Unternehmen dazu, ein Hinweisgebersystem einzurichten – am besten digital.

EU will Whistleblower schützen

Der Fall von Edward Snowden hat riesige Wellen geschlagen: Der ehemalige CIA- und NSA-Techniker brachte 2013 geheime Informationen über die Überwachungsmaßnahmen der US-Regierung an die Öffentlichkeit. Er deckte auf, dass die NSA mit Hilfe von Überwachungsprogrammen den Internetverkehr von Millionen von Menschen und sogar die Arbeit der US-Geheimdienste verfolgen kann. Snowden sah das als Verstoß gegen die Privatsphäre und sah sich gezwungen zu handeln. Das Ergebnis: Er wurde in den USA wegen Spionage angeklagt und steht auf der Fahndungsliste; er lebt in Russland im Exil.

Das Problem: Missstände aufzudecken, sollte eigentlich eine gute Sache sein. Whistleblowing kann in der Theorie nämlich dazu beitragen, Korruption, Diskriminierung und viele weitere Formen unrechtmäßigen Verhaltens zu bekämpfen. In einigen Fällen hat Whistleblowing auch in der Praxis zu wichtigen politischen oder gesellschaftlichen Veränderungen geführt. Fälle wie der von Edward Snowden haben allerdings eine enorm abschreckende Wirkung. Mit der Whistleblower-Richtlinie möchte die EU Hinweisgeber daher schützen – und die EU-Länder sind in der Pflicht, die Richtlinie mit Leben zu füllen. In Deutschland kommt man dieser Pflicht mit dem Hinweisgeberschutzgesetz nach.

Was ist das Hinweisgeberschutzgesetz?

Das Hinweisgeberschutzgesetz (HinSchG) ist am 2. Juli 2023 als deutsche Umsetzung der EU-Whistleblower-Richtlinie in Kraft getreten. Die Richtlinie sieht vor, dass EU-weit ein standardisierter Schutz für Hinweisgeber besteht. Dementsprechend regelt auch das deutsche HinSchG den Schutz von Personen, die im Rahmen ihrer beruflichen Tätigkeit einen Rechtsverstoß im Unternehmen entdeckt haben und diesen melden. Kern des Gesetzes ist, dass Hinweisgeber ohne Angst vor Repressalien Missstände offenlegen können müssen.

Das Gesetz soll aber nicht nur Hinweisgeber schützen, sondern auch die Vertrauenswürdigkeit von Unternehmen und der öffentlichen Verwaltung stärken: Wenn Mitarbeiter keine Angst vor Repressalien haben müssen, sind sie eher bereit, Missstände anzuzeigen; als Folge wären mehr Transparenz und ein verantwortungsvolleres Handeln seitens Unternehmen und Organisationen denkbar.

Unternehmen müssen aktiv werden

Für einen Großteil der Unternehmen bedeutet das Hinweisgeberschutzgesetz, aktiv werden zu müssen. Bereits seit dem 2. Juli 2023 sind Unternehmen mit mehr als 250 Mitarbeitern zur Umsetzung verpflichtet; seit

Digitales Hinweisgebersystem

Bei der Umsetzung eines digitalen Hinweisgebersystems bzw. einer Hintbox sollten die folgenden Punkte unbedingt berücksichtigt werden:

- Das Hinweisgebersystem sollte allgemeine Informationen zum Hinweisgeberschutzgesetz und zur Meldung von Verstößen bereithalten. Wer ist zu einer Meldung berechtigt? Was gibt es zu beachten? Wie wird mit Vertraulichkeit, Anonymität und Co. umgegangen? Wie wird die Meldung bearbeitet? Diese und weitere Fragen sollten beantwortet werden.
- Die Hintbox soll Mitarbeitern die Möglichkeit geben, alle relevanten Angaben zu machen – unter anderem zur Art des Verstoßes, zum Sachverhalt, zu Zeit und Ort des Geschehens, zu den beteiligten Personen und gegebenenfalls auch zu möglichen Beweisen.
- Hinweisgeber sollten auch die Option erhalten, persönliche Daten anzugeben. Die Anonymität ist in jedem Fall zu wahren. Im Zuge einer Strafverfolgung und einer eventuell benötigten Zeugenaussage wäre es grundsätzlich hilfreich, den Hinweisgeber kontaktieren zu können.
- Das Einverständnis des Mitarbeiters zur Weiterverarbeitung seiner Meldung ist unbedingt durch das digitale Hinweisgebersystem zu erfragen. Dabei sollte auch auf die geltende Datenschutzerklärung verwiesen werden.

dem 17. Dezember 2023 gilt die Pflicht aber auch für Unternehmen mit mehr als 50 Beschäftigten. Konkret geht es darum, eine interne oder externe Meldestelle einzurichten, über die Mitarbeiter Rechtsverstöße melden können. Bei einer internen Meldestelle ist eine Person oder eine Gruppe innerhalb des Unternehmens zuständig; die externe Meldestelle wird von einem externen Dienstleister betrieben. Sie ist in der Regel teurer als eine interne Meldestelle, gilt dafür aber als unabhängiger von unternehmensinternen Interessen.

Für welche Variante sich Unternehmen entscheiden, bleibt ihnen selbst überlassen. Beide Varianten lassen sich auch auf verschiedene Arten umsetzen. Intern könnte beispielsweise eine Vertrauensperson dafür zuständig sein, Meldungen entgegenzunehmen – natürlich mit der Maßgabe, diese vertraulich zu behandeln. Auch eine interne oder externe Telefonhotline wäre denkbar. Am besten eignet sich aber ein elektronisches Meldesystem als Hinweisgebersystem.

Hinweise digital abgeben

Ein digitales Hinweisgebersystem (auch: Hintbox-Plattform) ist ein Online-Tool, das es Mitarbeitern ermöglicht, Hinweise auf Rechtsverstöße zu melden. Es bietet eine sichere und vertrauliche Möglichkeit, Hinweise einzureichen, auf Wunsch auch anonym. Bei dem Hintbox-System kann es sich beispielsweise um ein Formular handeln, das Mitarbeiter über einen sicheren Link oder eine App erreichen. Welche Inhalte so ein Tool haben sollte, sehen Sie oben in der Infobox.

Sollten auch in Ihrem Unternehmen mehr als 50 Mitarbeiter beschäftigt sein, sind auch Sie gefordert, ein (digitales) Hinweisgebersystem einzurichten. Es gibt in Ihrem Unternehmen keinen Mitarbeiter, der sich einerseits mit den genauen rechtlichen Vorgaben, andererseits mit dem Aufsetzen eines (digitalen) Hinweisgebersystems auskennt? Dann sprechen Sie uns an: Wir stehen Ihnen natürlich gern zur Seite und beraten Sie zu den Umsetzungsmöglichkeiten!

Cookie-Banner: nervig aber notwendig

Fast jedes Unternehmen ist mit einer eigenen Webseite im World Wide Web vertreten. Und nahezu jede Webseite setzt auf Cookies, um Nutzern mehr Komfort und ein positives Nutzererlebnis bieten zu können. Das Problem: Ein Cookie-Hinweis ist in diesem Fall Pflicht!

Was sind eigentlich Cookies?
Cookies sind kleine Textdateien oder Datenpakete, die vorübergehend im Browser von Internetnutzern gespeichert werden und Informationen über sie erheben. Sie helfen Webseiten dabei, Nutzereinstellungen zu behalten, die Anmeldung zu erleichtern und personalisierte Inhalte bereitzustellen. Das Nutzererlebnis soll dadurch so angenehm wie möglich gestaltet werden. Ein Beispiel ist das Onlineshopping: Mit Hilfe von Cookies füllt sich der Warenkorb nach und nach, während ungestört weiter gestöbert wird. Für die Funktion der Webseite ist diese Art von Cookie daher auch essentiell.

Das Problem: Cookies ermöglichen es Webseitenbetreibern auch, Nutzungsstatistiken zu erstellen und Rückschlüsse auf Verhalten und Interessen der Nutzer zu ziehen, was unter anderem für gezielte Werbemaßnahmen genutzt werden kann. Diese Art von Cookies ist für die Funktion von Webseiten nicht notwendig, verrät unter Umständen aber viel über den jeweiligen Seitenbesucher. Und da es hier um personenbezogene Daten geht, hat unter anderem der Datenschutz ein Wörtchen mitzureden.

Cookie-Banner sind Pflicht
Die DSGVO, die ePrivacy-Verordnung und das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) verpflichten Webseitenbetreiber dazu, die Zustimmung der Nutzer einzuholen, bevor sie Cookies setzen. Umgesetzt wird dies meist durch ein Cookie-Banner, das beim Aufruf einer Webseite direkt aufploppt. Das Pop-up-Fenster soll Besuchern die Möglichkeit geben, festzulegen, welcher Art von Cookies sie ihre Zustimmung geben.

Da aber so ziemlich jede Webseite ihre Besucher mit einem Cookie-Banner konfrontiert, ist aus der eigentlich sinnvollen Schutzmaßnahme ein ein lästiges – aber notwendiges – Übel geworden. Für viele Internetnutzer sind die permanente Zustimmungspflicht und das ständige Fragen nach »Ablehnen« oder »Akzeptieren« von Cookies eine unerwünschte Unterbrechung, die das Surferlebnis stört. Vor allem dann, wenn Cookie-Banner – bewusst oder unbewusst – benutzerunfreundlich gestaltet sind. Das Ergebnis: Der Cookie-Verwendung wird rasch zugestimmt, ohne dass sich Nutzer der eigentlichen Tragweite bewusst sind.

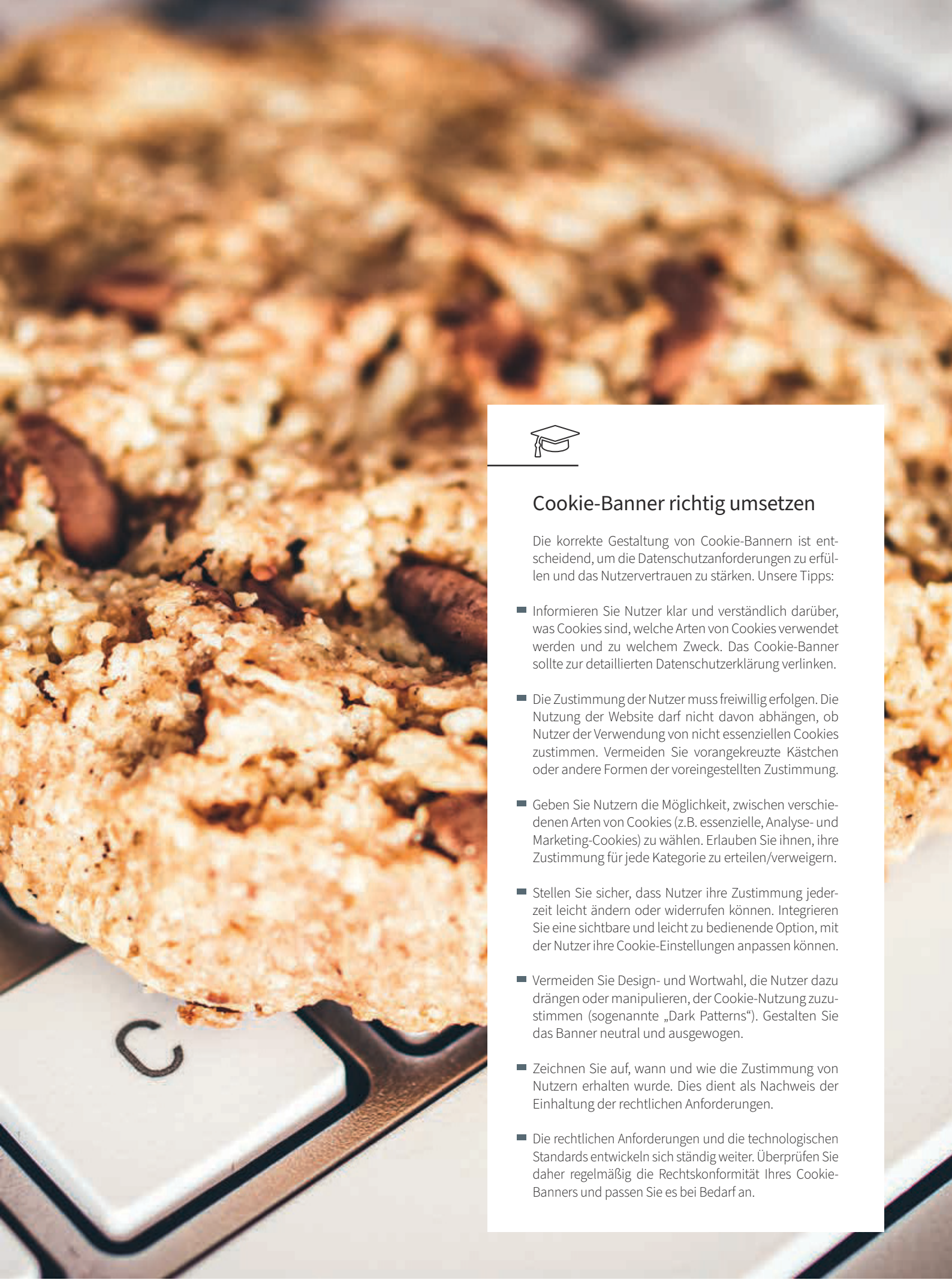
Die EU-Kommission plant daher, gegen die »Cookie-Müdigkeit« vorzugehen und die Zustimmungsverfahren zu vereinfachen. Verbraucher sollen durch die Initiative seltener und verständlicher über Cookies informiert werden und sich bewusster für oder gegen die Nutzung entscheiden können.

Zwischen Notwendigkeit & Nervfaktor
Die Initiative könnte die ohnehin schon komplexen rechtlichen Anforderungen bezüglich der Cookie-Verwendung aber noch komplizierter machen. Auch KMU sind als Betreiber von Webseiten wieder einmal gefordert: Die Nichtbeachtung der Cookie-Richtlinie kann andernfalls nämlich zu zu erheblichen Sanktionen führen. Bei einem Verstoß gegen die Vorgaben der Cookie-Richtlinie drohen nicht nur Bußgelder, die je nach Schwere des Verstoßes und dem jährlichen Umsatz in die Millionen gehen können, sondern auch Vertrauensverluste bei Kunden und Nutzern.

Die Einhaltung der gesetzlichen Vorgaben zu Cookies ist ein komplexes Unterfangen, das spezifisches Wissen erfordert. Hier kommen IT-Dienstleister ins Spiel! Gern unterstützen wir bei der Gestaltung von Cookie-Bannern, die den gesetzlichen Anforderungen entsprechen und für Nutzer verständlich sind.

Denken Sie an die Datenschutzerklärung!

Sofern auf einer Webseite personenbezogene Daten erhoben, übermittelt, verarbeitet oder genutzt werden, ist eine DSGVO-konforme Datenschutzerklärung ein Muss. Typische personenbezogene Daten, die bei Webseitenbesuchen erhoben werden können, sind IP-Adresse, E-Mail-Adresse, Standortdaten, Name, Alter und Anschrift. Die Erklärung sollte Webseitenbesucher verständlich und transparent darüber aufklären, wie mit solchen Daten umgegangen wird. Unternehmen, die trotz der Verarbeitung personenbezogener Daten auf eine Datenschutzerklärung verzichten, drohen Abmahnungen, Geldbußen und Schadensersatzforderungen. Sanktionen sind aber auch bei fehlerhaften oder unvollständigen Datenschutzerklärungen möglich. Daher gilt: Gehen Sie gewissenhaft mit diesem Thema um!



Cookie-Banner richtig umsetzen

Die korrekte Gestaltung von Cookie-Bannern ist entscheidend, um die Datenschutzanforderungen zu erfüllen und das Nutzervertrauen zu stärken. Unsere Tipps:

- Informieren Sie Nutzer klar und verständlich darüber, was Cookies sind, welche Arten von Cookies verwendet werden und zu welchem Zweck. Das Cookie-Banner sollte zur detaillierten Datenschutzerklärung verlinken.
- Die Zustimmung der Nutzer muss freiwillig erfolgen. Die Nutzung der Website darf nicht davon abhängen, ob Nutzer der Verwendung von nicht essenziellen Cookies zustimmen. Vermeiden Sie vorangekreuzte Kästchen oder andere Formen der voreingestellten Zustimmung.
- Geben Sie Nutzern die Möglichkeit, zwischen verschiedenen Arten von Cookies (z.B. essenzielle, Analyse- und Marketing-Cookies) zu wählen. Erlauben Sie ihnen, ihre Zustimmung für jede Kategorie zu erteilen/verweigern.
- Stellen Sie sicher, dass Nutzer ihre Zustimmung jederzeit leicht ändern oder widerrufen können. Integrieren Sie eine sichtbare und leicht zu bedienende Option, mit der Nutzer ihre Cookie-Einstellungen anpassen können.
- Vermeiden Sie Design- und Wortwahl, die Nutzer dazu drängen oder manipulieren, der Cookie-Nutzung zuzustimmen (sogenannte „Dark Patterns“). Gestalten Sie das Banner neutral und ausgewogen.
- Zeichnen Sie auf, wann und wie die Zustimmung von Nutzern erhalten wurde. Dies dient als Nachweis der Einhaltung der rechtlichen Anforderungen.
- Die rechtlichen Anforderungen und die technologischen Standards entwickeln sich ständig weiter. Überprüfen Sie daher regelmäßig die Rechtskonformität Ihres Cookie-Banners und passen Sie es bei Bedarf an.

ÜBERREICHT DURCH

edvXpert GmbH

Von-Hünefeld-Str. 1
50829 Köln

Telefon +49 221 669911-0
E-Mail info@edvxpert.de

http://www.edvxpert.de/