

Podcast Aufzeichnung in Textform

Thema Datenschutz und Rechenschaftspflicht

Zwei Personen unterhalten sich zum Thema Rechenschaftspflicht.

Genau. Und das ist wirklich zentral. Rechenschaftspflicht heißt ja nicht nur, die Regeln zu kennen, sondern sie müssen als Unternehmen jederzeit, ja wirklich jederzeit, nachweisen können, dass sie sich daranhalten.

Nachweisen können. Das ist der Knackpunkt.

Richtig. Und das muss dokumentiert sein, die Quellen betonen das ja auch, Behörden können das prüfen, jederzeit auch mal ohne Ankündigung.

Okay d.h. vorbereitet sein ist alles. Wie stellt man das denn sicher, also, dass man diesen Nachweis auch wirklich führen kann, wenn es drauf ankommt? Ihre Unterlagen nennen da ja ein paar Punkte, ja, da gibt es mehrere Säulen, sozusagen. Erstens, ganz wichtig: regelmäßige, interne Audits, die „macht“ der Datenschutzbeauftragte, der DSB schreibt darüber Berichte, das ist ein Kernnachweis. Und zweitens, eng damit verbunden das ganze Datenschutz-System, also alle Dokumente müssen aktuell gehalten werden. Immer. Veraltete Doku, das kann laut dem Text hier schnell teuer werden. Bußgelder drohen.

Verstehe. Also kein Ordner, der im Schrank verstaubt, sondern ein lebendes System. Das ist schon mal wichtig, festzuhalten. Was gehört noch dazu? Es geht ja nicht nur um Papier.

Nein, genau. Drittens: Begehungen. Wirklich mal durch die Büros gehen, schauen, wo vielleicht Schwachstellen am Arbeitsplatz sind und das auch festhalten.

Ah, okay. Die physische Umgebung.

Richtig. Und viertens die Leute schulen, die Beschäftigten müssen wissen, worum es geht und auch das muss man nachweisen können, wer wann geschult wurde. Interessant ist ja der Hinweis im Text, dass bei Neuen (Beschäftigten) sogar eine schnelle Grundausbildung gefordert wird. Online geht das wohl ganz gut.

Okay. Prozesse, Orte, Menschen, logisch. Und die digitale Visitenkarte, die Website, die sich auch im Thema.

Punkt fünf, die Website überwachen und bewerten. Hier gibt's ne wichtige Ansage im Text. Der DSB muss Bescheid wissen, bevor sie was an der Website ändern. Sonst kann er ja gar nicht prüfen, ob das passt.

Ah, okay. Der muss also frühzeitig rein.

Genau, und das führt zum sechsten Punkt, die IT-Sicherheit. Die muss sich ja ständig weiter entwickeln, und das am besten zusammen mit dem DSB. Änderungen bei der Datenverarbeitung, so steht hier, müssen unverzüglich dokumentiert werden.

Unverzüglich, puh stressig.

Ja, das unterstreicht die Dringlichkeit. Datenschutz darf halt kein nachträgliches aufräumen sein, sondern muss sofort mitgedacht und dokumentiert werden, wenn sich was Relevantes ändert, die Nachweiskette darf nicht abreißen.

Diese Kontinuität, dieser Fluss, zieht sich durch. Es ist auch von festen Termin die Rede in den Unterlagen, oder? Für Updates und Audits?

Korrekt. Für die System-Aktualisierung, also für die Dokumente und Prozesse werden mindestens zwei Termine pro Jahr empfohlen. Die internen Audits, die haben auch einen Rhythmus. Jährlich bei bis zu 20 Leuten. Bei größeren Firmen können auch unterjährig weitere Termine oder zumindest mal Gespräche nötig werden.

Und wer stößt an? Der DSB.

Der DSB muss die Termine zwar überwachen, das ist seine Pflicht, aber die Initiative, die Planung, die liegt beim Unternehmen selbst, also bei Ihnen.

Das heißt also für Sie in der Praxis: nicht warten, bis der DSB anklopft, sondern selber aktiv werden. Diese wiederkehrenden Termine, Audits, Updates, fest einplanen. Der Tipp hier ist ja, die (Termine) etwa ein Monat vorher festzumachen. Man kann sich ja an den Vorjahresterminen orientieren. Gut. Fassen wir vielleicht noch mal zusammen, was ihre Quellen uns damit geben: DSGVO Konformität ist keine einmalige Sache, sondern ein dynamischer Prozess, ständige Aufmerksamkeit, lückenlose Doku und eben diese proaktiven Planungen sind nötig. Und im Zentrum diese Rechenschaftspflicht.

Es reicht eben nicht, die Regeln eben nur zu befolgen, springende Punkt, das macht Art. 5 und auch ihre Unterlagen klar, ist: sie müssen es im Zweifel auch beweisen können. Lückenlos. Diese Beweisbarkeit, das ist die harte Währung im Datenschutz.

Die Beweisbarkeit, ein gutes Stichwort zum Schluss. Und damit vielleicht eine Frage, die Sie einfach mal für sich mitnehmen: Wenn morgen früh die Aufsichtsbehörde, ohne Anmeldung bei Ihnen auf der Matte stünde, wären sie wirklich sicher, sofort alles lückenlos belegen zu können?