KI und Datenschutz

KI und Datenschutz, ein Thema, das im Moment wirklich jeden betrifft. Lasst uns mal reinschauen, was ihr da jetzt unbedingt wissen müsst, gerade hier bei uns in Deutschland. Also mal ganz ehrlich, wer von euch nutzt bei der Arbeit nicht schon längst Tools wie ChatGPT, Copilot oder vielleicht die KI Funktion von Adobe? Ich wette, das sind so einige. Und genau da, genau da wirds spannend in Sachen Datenschutz, denn sobald ihr über diese Tools auch nur irgendwas verarbeitet, was mit Personen zu tun hat, also sagen wir mal Namen, E-Mailadressen, Kundendaten, dann seid ihr mittendrin und zwar in der Datenschutzgrundverordnung. Genau, der guten alten DSGVO. Okay, also wie sieht die rechtliche Lage da jetzt genau aus? Wichtig ist, wir reden hier nicht über irgendein brandneues KI Gesetz. Nein, die Basis für alles, was mit Daten in KI Systemen passiert, ist und bleibt die DSGVO, die wir ja schon kennen. Und da kommt jetzt oft die Frage, was ist denn mit dem AI Act? Ganz wichtig zu verstehen. Der AI Act, der kommt oben drauf. Der ersetzt die DSGVO nicht. Stellt es euch so vor, die DSGVO ist das Fundament für alle personenbezogenen Daten und der AI Act, der packt dann noch mal spezielle Regeln für die Risiken drauf, die nur von der KI selbst kommen. Also Ergänzung, kein Ersatz. Und genau das führt uns zu den Risiken und die sind, na ja, manchmal ziemlich gut versteckt, denn die Kombi aus KI und Datenschutz, die hats echt in sich und birgt ein paar ziemlich knifflige Fallen. Also, wir denken ja oft nur an Namen oder E-Mailadressen oder, aber es geht viel weiter. Nehmt mal eine simple Nutzer-ID, die sieht erstmal total anonym aus, aber wenn ihr irgendwo eine Liste habt, wo diese ID einem Kundennamen zugeordnet ist, zack, schon ist diese ID ein personenbezogenes Datum. Allein die Möglichkeit der Kombination reicht aus. Und jetzt kommt der Punkt, wo es wirklich heikel wird. Die sensiblen Daten, die gebt oft ihr selbst in die KI ein. Völlig unbewusst. Denkt mal drüber nach. Ihr tippt schnell einen Prompt wie: Hey, fass mal die Mail von Kunde Müller zum Projekt XY zusammen. Bum. In dem Moment habt ihr personenbezogene Daten direkt ins System geschickt. Einfacher gehts kaum. Tja, und das führt uns zum wohl größten Problem im ganzen DSGVO Kontext, dem Recht auf Löschung. Stellt euch vor, die Daten wurden einmal zum Trainieren der KI genutzt, dann sind die nicht einfach wie eine Datei in einem Ordner gespeichert. Nein, die sind quasi ins Gehirn des Modells eingebrannt. Die da wieder rauszupicken ist technisch extrem schwierig, wenn nicht sogar unmöglich. Das Recht auf vergessen werden, puh, das wird da zu einer echten Mammutaufgabe. Okay, das klingt jetzt vielleicht alles ein bisschen düster, aber keine Panik. Ihr seid dem Ganzen nicht hilflos ausgeliefert. Im Gegenteil, es gibt ganz konkrete Schritte, mit denen ihr die Kontrolle behalten könnt. Und genau dafür haben wir jetzt eine Checkliste für euch. Die große Frage ist also, was genau

könnt ihr jetzt tun, um auf der sicheren Seite zu bleiben? Also, passt auf, hier sind vier wirklich entscheidende Punkte. Erstens, macht mal eine Bestandsaufnahme. Können in den KI Systemen, die ihr nutzt, überhaupt personenbezogene Daten landen. Zweitens, seid mega vorsichtig bei Cloud Tools wie Copilot. Alles, was ihr da eingebt, geht an fremde Server und ganz wichtig, die Verantwortung dafür, die bleibt bei euch. Drittens, und das ist vielleicht der wichtigste Tipp überhaupt, verbietet der KI eure Daten zum Training zu nutzen. Schaut mal in die Einstellung, da gibts meistens einen Haken, den ihr entfernen könnt. Und viertens, wenn es gar nicht anders geht und ihr personenbezogene Daten nutzen müsst, dann lest die AGBs des Anbieters und checkt, ob das alles mit der DSGVO klar geht. Und für alle, die jetzt noch tiefer einsteigen wollen, habe ich einen echten Tipp. Der Digitalverband Bitcom hat dazu einen super Praxisleitfaden rausgebracht. Der ist wirklich gold wert, wenn ihr eine vollständige Checkliste braucht. Also am Ende des Tages läuft alles auf diese eine ganz simple Frage hinaus. Wisst ihr wirklich, was die KI, die ihr jeden Tag benutzt, mit euren Daten macht und noch wichtiger mit den Daten eurer Kunden? Denn die Antwort auf diese Frage, die entscheidet am Ende über Vertrauen, Sicherheit und ja auch über empfindliche Bußgelder.