www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

Rechtssicher | vollständig | dauerhaft

September 2025

Bild: iStock.com/Funtap

Für Datenschutzbeauftragte kann es eine Herausforderung sein, sich den Überblick über alle digitalen Benutzerzugänge im Unternehmen zu verschaffen. Einblick in die Lösung zur Passwortverwaltung kann hier wertvolle Hilfe leisten.

Benutzerzugänge zuverlässig erfassen

Datenschutz und die Benutzerverwaltung

In vielen Unternehmen fehlt eine umfassende zentrale Übersicht über alle Benutzerzugänge. Die Betonung liegt auf „alle". Ich habe mir angewöhnt, bei Kunden genau das nachzufragen – gibt es eine zentrale Benutzerverwaltung? Die Antwort ist erschreckend oft ausweichend oder ein klares Nein. Was lässt sich dagegen tun?

Beschäftigte Personen müssen mit ihnen zugeordneten Berechtigungen die Tätigkeiten erledigen, für die sie zuständig sind. Dabei sind verschiedene Systeme zu nutzen und definierte Regeln einzuhalten. Allerdings dürfen hierbei ausschließlich die Berechtigungen zugeordnet sein, die objektiv erforderlich sind (Erforderlichkeit).

Die Datenverarbeitungen dürfen nur die Personen durchführen, die dafür zuständig sind. Diese Personen dürfen die Daten und Informationen nur in einer Weise weitergeben, wie es ihre Tätigkeit vorgibt (Vertraulichkeit). Die Daten und Informationen müssen zudem dann zur Verfügung stehen, wenn dies für die Arbeit notwendig ist (Verfügbarkeit).

Die Änderung von Daten und Informationen darf nur befugt erfolgen, also wenn dies im Rahmen der Tätigkeit unumgänglich ist (Integrität).

Nutzen der Benutzerverwaltung für digitale Systeme

Damit dies alles in digitalen Systemen möglich ist, gibt es die Benutzerverwaltung. Diese ist ein zentraler Bestandteil der digitalen Arbeit. Die Benutzerverwaltung regelt insbesondere,

- wer (welche Person oder Rolle)
- welche Daten (Art und Umfang)
- mit welchen Systemen (Applikationen, Servern, Datenbanken)
- unter welchen Bedingungen (z.B. Ort, Zeit, Arbeitsgerät)
- für welchen Zweck

verarbeiten darf. →

Editorial

Ricarda Veidt, Chefredakteurin

Augen auf beim KI-Kauf

Liebe Leserin, lieber Leser! Hatten Sie auch schon die Situation, dass jemand in einem Online-Meeting vorgeschlagen hat, das lästige Protokoll doch die KI erledigen zu lassen? In einem solchen Termin, den ich erlebt habe, war die Reaktion einhellige Ablehnung. Denn wer weiß denn ohne genaue Prüfung schon, was mit den Daten passiert? Unser Beitrag zu den sog. „Notetakern" macht deutlich, worauf Sie achten müssen.

Geht es darum, eine neue KI-Anwendung anzuschaffen und zu prüfen, ist allerdings eine ganz zentrale Frage: Handelt es sich überhaupt um KI? Das „AI-Washing" greift immer weiter um sich. Wo KI draufsteht, muss also nicht KI drin sein. Augen auf beim KI-Kauf ...

Angesichts der zahlreichen KI-Themen, die sicher auf Ihrem Schreibtisch liegen, gilt es aber, die „Standards" nicht zu vernachlässigen. Benutzerverwaltung, Prüfung von Videoüberwachung, der Dauerbrenner Cookies – bei all diesen Themen ist Ihre Beratung und Überwachung gefragt. Daher lesen Sie auch in dieser Ausgabe nicht nur Beiträge, die sich mit KI befassen.

Eine anregende Lektüre
wünscht Ihre Ricarda Veidt

Aufgabe von Datenschutzbeauftragten

Datenschutzbeauftragte (DSB) sind verpflichtet, zu überwachen, welche Daten Beschäftigte im Unternehmen verarbeiten und ob dies im Einklang mit den Datenschutzgrundsätzen geschieht.

Je weiter die Digitalisierung voranschreitet, desto komplexer fällt diese Aufgabe aus. Die folgenden Fragen gewinnen zunehmend an Bedeutung, und die Antworten fallen nicht immer leicht:

- Wie erhält man eine zutreffende Übersicht über alle Systeme und Systemzugänge?
- Wo befinden sich die Daten, wer verarbeitet sie wofür und unter welchen Bedingungen und wer kontrolliert dies?
- Welche Maßnahmen stellen sicher, Berechtigungen nachvollziehbar und risikominimierend zu vergeben – und auch wieder zu entziehen?

In der Praxis gestaltet sich die Suche nach den Antworten oftmals schwieriger als erwartet. Institutionen wie Unternehmen setzen eine Vielzahl von Systemen und Anwendungen ein: klassische IT-Systeme, spezialisierte Fachanwendungen, Produktionssteuerungen, mobile Apps und cloudbasierte Plattformen. Die Brücke, die all diese Systeme miteinander verbinden und kontrollierbar machen soll, ist die Benutzerverwaltung. Damit lässt sich steuern, wer welche Systeme nutzen darf, unter welchen Bedingungen und mit welchen Rechten.

Die Benutzerverwaltung ist somit ein zentrales Prüffeld für DSB – und zugleich eine Herausforderung, wenn sie über viele Systeme und Plattformen hinweg verteilt ist.

Verzeichnisdienste als Rückgrat

Fragt man die IT-Abteilung nach einer Übersicht der Benutzer und Zugänge, verweist sie häufig auf das Active Directory (AD) oder ein vergleichbares Verzeichnisdienstsystem.

Das Active Directory ist ein Dienst, der Benutzerkonten, Rechner, Server und Anwendungen in einer zentralen Struktur verwaltet. Es erlaubt, Benutzerrollen zu definieren, Berechtigungen zu steuern und Anmeldeprozesse zu organisieren. In der klassischen IT-Umgebung ist das AD das zentrale Rückgrat für die Verwaltung von Benutzerrechten. Typische Aufgaben und Merkmale des Active Directory sind:

- Benutzer und Gruppen zentral verwalten
- Zugriffsrechte auf Server, Anwendungen und Datenbanken steuern
- Vorgaben für Passwortregeln und Anmeldebedingungen festlegen
- Berechtigungen über Gruppenmitgliedschaften vererben
- Anmeldevorgänge und Berechtigungsänderungen protokollieren

Auf den ersten Blick scheint das AD die perfekte Antwort auf die Frage nach der Übersicht der Benutzerzugänge zu sein.

Die Lücke zwischen Anspruch und Realität

Bei genauerer Betrachtung zeigt sich jedoch schnell: Das Active Directory erfasst längst nicht alle Systeme und Datenverarbeitungen, die im Unternehmen existieren. Typische Bereiche, die oft nicht oder nur unvollständig im AD abgebildet sind:

- Produktionssysteme (OT): Viele Maschinen- und Steuerungssysteme arbeiten mit eigenen Benutzerverwaltungen, völlig getrennt vom zentralen Verzeichnisdienst.
- Spezialanwendungen: Fachspezifische Softwarelösungen, etwa in der Entwicklung, im Controlling oder im technischen Service, haben oft eigene Benutzerkonten und Zugriffskonzepte.
- Cloud-Dienste: SaaS-Anwendungen wie spezialisierte Plattformen für Projektmanagement, Zeiterfassung oder Kommunikation laufen häufig unabhängig vom AD.
- Mobile Geräte und Apps: Zugriffe über Tablets, Smartphones oder mobile Applikationen sind oft nicht oder nur eingeschränkt im AD verwaltet.
- Externe Partner und Dienstleister: Temporäre Zugänge erhalten Wartungsfirmen, Berater oder Freelancer oft ad hoc. Sie sind nicht sauber ins zentrale Verzeichnis integriert.

Für DSB ergibt sich daraus die Herausforderung, bei der Überprüfung der Benutzerverwaltung nicht nur auf das AD zu vertrauen, sondern die gesamten Strukturen der digitalen Arbeitsumgebungen einzubeziehen.

Benutzerkonten sind mehr als eine E-Mail-Adresse

Die meisten Zeitgenossen gehen davon aus, dass heute alle beschäftigten Personen in einem Unternehmen über eine eigene E-Mail-Adresse verfügen. Das führt zu der vermeintlich logischen, aber falschen Auffassung, dass man nur eine Übersicht über alle E-Mail-Adressen erstellen müsse, und alle Mitarbeitenden seien erfasst.

Tatsächlich haben bei Weitem nicht alle beschäftigten Personen eine eigene E-Mail-Adresse. Es gibt zahlreiche Arbeitsbereiche, in denen Beschäftigte zwar ein Benutzerkonto, aber keine persönliche E-Mail-Adresse benötigen, etwa in Produktion und Fertigung. Sie brauchen lediglich einen Zugang zu Maschinensteuerungen oder zu Qualitätsmanagementsystemen. Bei der Arbeit in Logistik und Lager haben Mitarbeitende Zugriff auf Lagerverwaltungssysteme oder auf Scanner. Dazu ist eine E-Mail-Adresse ebenfalls nicht unbedingt erforderlich. Das gilt auch für Verkauf und Kasse. Sie nutzen Kassensysteme mit persönlicher Anmeldung, aber ohne E-Mail-Adresse. Ähnliches gilt für viele weitere Bereiche.

Funktion von Benutzerkonten

Alle diese Beschäftigten benötigen Benutzerkonten. Diese dienen dazu, Personen individuell zu identifizieren und ihnen gezielt Berechtigungen zuzuweisen.

Meine Beobachtung ist hier, dass viele DSB sich darüber noch keine oder nur wenige Gedanken gemacht haben. Das ist nicht nur ein Thema des Datenschutzes, sondern zunehmend auch der Security. Immer öfter laufen Angriffe über Benutzerkonten, die deutlich schlechter abgesichert sind als die Verzeichnisdienste, bei denen die meisten davon ausgehen, dass diese die einzigen legitimierenden Zugänge zu Daten von Unternehmen darstellen.

Es gilt also, zunächst einmal festzustellen, welche und wie viele Benutzerkonten vorhanden sind und ob diese den Anforderungen des Datenschutzes genügen.

IT und OT

Erschwerend kommt hinzu, dass im Unternehmensalltag oft zwei Welten existieren. Zur IT (Information Technology) gehören Informationssysteme wie Rechner, Server, Netzwerke und Anwendungen zur Datenverarbeitung – also alles, was im Büro oder im digitalen Geschäftsverkehr zum Einsatz kommt. Hier verorten die meisten die Hauptanwendung des Datenschutzes.

Doch zudem gibt es die OT (Operational Technology). OT bezeichnet technische Systeme, die physische Prozesse steuern oder überwachen, wie Maschinen, Produktionsanlagen oder Gebäudetechnik.

Historisch gesehen waren IT und OT streng getrennt: IT diente der Datenverarbeitung, OT der Prozesssteuerung. Erst durch die Digitalisierung, Stichwörter Industrie 4.0 und IoT (Internet of Things), wachsen beide Bereiche zunehmend zusammen – mit neuen Herausforderungen für Sicherheit und Datenschutz.

In der Produktion haben insbesondere Führungskräfte oft sowohl IT- als auch OT-Zugänge. Über die IT erfolgt der Zugriff auf klassische Systeme wie das E-Mail-Postfach, das Intranet, ERP- (Enterprise Resource Planning) oder Zeiterfassungssysteme, etwa um Schichtpläne einzusehen, Urlaubsanträge zu bearbeiten oder Produktionsdaten auszuwerten.

Gleichzeitig nutzt dieselbe Person OT-Zugänge für die Maschinensteuerung, um Produktionslinien zu überwachen oder Wartungsarbeiten über spezialisierte Terminals durchzuführen. Diese OT-Systeme sind häufig direkt mit Anlagen verbunden und haben eigene Anmeldeverfahren, die sich deutlich von den IT-Standards unterscheiden. Während die Verwaltung der IT-Zugänge meist durch zentrale Benutzerverzeichnisse erfolgt, sind OT-Zugänge oft historisch gewachsen, lokal eingerichtet und weniger streng gesichert.

Glücksfall Passwortverwaltung

Gibt es in dem Unternehmen eine Passwortverwaltung? Wenn ja, haben Sie als DSB sich die Passwortverwaltung einmal näher angesehen? Im Idealfall betrifft diese IT und OT.

Passwortverwaltungen ermöglichen es, komplexe und individuelle Passwörter für jedes System sicher zu speichern und automatisch bereitzustellen. Damit entfällt die unsichere Praxis, Passwörter mehrfach zu verwenden oder auf Zetteln und in ungeschützten Dateien zu notieren.

Bei den meisten professionellen Passwortverwaltungen bleibt erkennbar, für wie viele Systeme oder Konten ein Passwort gespeichert ist. Nutzer können ihre gespeicherten Einträge in einer strukturierten Übersicht einsehen – häufig nach Kategorien sortiert wie „IT-Systeme“, →

„Produktionsanlagen“, „Cloud-Dienste“ oder „interne Anwendungen“. So bleibt nachvollziehbar, wo Zugangsdaten im Einsatz sind.

Passwortmanager können IT- und OT-Zugänge gleichermaßen erfassen, strukturieren und nach Sicherheitsstandards wie Passwortstärke und Änderungszyklen verwalten. Das erleichtert nicht nur die Arbeit der Beschäftigten, sondern unterstützt auch DSB und IT-Sicherheitsbeauftragte dabei, ihren Prüfpflichten nachzukommen.

Sie bieten die Möglichkeit, alle Benutzerzugänge systematisch zu erfassen und strukturiert zu verwalten, ohne auf personenbezogene Informationen aus HR-Systemen (Human Resources) zuzugreifen. In der Passwortverwaltung findet sich lediglich der Vermerk, welcher Zugang zu welchem System besteht und welches Passwort dazu gehört – nicht aber die personalrechtlichen Daten.

PRAXIS-TIPP

Überprüfen Sie, ob alle gespeicherten Passwörter aktuell sind, ob die zugehörigen Systeme noch zum Einsatz kommen und ob die Sicherheitseinstellungen wie Passwortstärke und Änderungszyklen angemessen sind. So bleiben Übersicht, Datenschutz und IT-Sicherheit gewährleistet.

Ein Passwortmanager als Teil der Benutzerverwaltung ermöglicht dem DSB, die folgenden Aufgaben zu bewältigen:

- Überflüssige oder veraltete Zugänge identifizieren: Gibt es Konten, die zu deaktivieren oder zu löschen sind?
- Erfordernis: Benötigen die Nutzenden tatsächlich alle Benutzerzugänge? Mitunter kommt im Laufe der Zeit einiges zusammen, was nicht mehr passt.
- Stichprobenartige Überprüfungen: Sind die hinterlegten Passwörter ausreichend sicher (Länge, Sonderzeichen etc.)?
- Frequenz der Passwortwechsel überwachen: Ändert man die Passwörter regelmäßig und entsprechen sie den Anforderungen an Komplexität und Sicherheit?
- Mehrfachverwendungen erkennen: Kommen dieselben Passwörter für verschiedene Systeme zum Einsatz, was ein Sicherheitsrisiko darstellt?
- Nachvollziehbarkeit: Lassen sich Zugänge bestimmten Rollen oder Personen im Betrieb eindeutig zuordnen, ohne dabei die HR-Daten zu kompromittieren?

Fazit

Eine vollständige Übersicht über alle Benutzerzugänge ist eine Voraussetzung für Datenschutz und Informationssicherheit, die gerade an der Schnittstelle zwischen IT und OT nicht offensichtlich ist.

Da die Benutzerverwaltung für IT und OT oft getrennt organisiert ist, kann man auf den Trick mit der Passwortverwaltung zurückgreifen. Passwortmanager ermöglichen die gewünschte Transparenz, wo HR-Systeme naturgemäß an ihre Grenzen stoßen. Die nähere Betrachtung der Passwortmanager unterstützt DSB bei der Überwachung gemäß Art. 39 DSGVO (Datenschutz-Grundverordnung) und hilft Unternehmen dabei, Benutzerkonten sicher, nachvollziehbar und effizient zu verwalten.

Beispiele aus der Praxis

Beispiel 1: Ein Produktionsleiter hat Benutzerzugänge für das Schichtplanungssystem, die Maschinenwartung, das Gebäudemanagement und das zentrale Intranet. Über den Passwortmanager lassen sich diese Konten sichtbar machen und prüfen, ob die Passwörter stark und einzigartig sind.
Beispiel 2: Ein Techniker hat Zugriff auf drei verschiedene Produktionsanlagen und eine mobile Wartungs-App. Mit der Passwortverwaltung lässt sich sicherstellen, dass die Passwörter unterschiedlich und sicher sind – und dass veraltete Anlagenkonten nach Wartungsende erlöschen.
Beispiel 3: Eine Schichtaufsicht hat ein Konto für die Alarmierung bei Störungen und zusätzlich Zugriff auf das Meldesystem für Qualitätsabweichungen. Der Passwortmanager zeigt auf, ob beide Zugänge aktuell gepflegt und gegen Fremdzugriffe abgesichert sind.

WICHTIG

Es geht nicht darum, die Passwörter für die Anwendungen zu sichten, sondern es geht um die hier gezeigten Prüfungen, die in einer sicheren Passwortverwaltung auch ohne Kenntnis der Passwörter erfolgen kann.

Eberhard Häcker ist Geschäftsführer der TDSSG GmbH und seit vielen Jahren als Datenschutzberater sowie externer Datenschutzbeauftragter tätig.

Bild: iStock.com/iLexx

Bei Online-Videokonferenzen wie auch bei Tools für deren KI-gestützte Protokollierung kann die Datenübertragung in Drittländer datenschutzrechtliche Probleme aufwerfen

Vorsicht Falle!

KI-Protokolle von Videokonferenzen

Ist es nicht wunderbar, dass wir keine Protokolle von Videokonferenzen manuell erstellen müssen? Schließlich gibt es tolle „Notetaker"-Tools, die uns die Arbeit abnehmen – einfach topp! Doch die Werkzeuge bergen Datenschutztücken.

Macht sich jemand Gedanken, wohin die Informationen, die Sprache, die Bilder gehen und was mit dem Datenpaket veranstaltet wird, das ein „Notetaker" (digitaler Schriftführer) erfasst? In der Regel nein. Es ist wie immer im Leben: Wenn uns ein schönes und durchaus nützliches Produkt auf den Schreibtisch oder vor die berühmten Füße fällt, dann nehmen wir es einfach. Das Tool ist in das Videokonferenzsystem integriert und auch noch kostenlos, das passt dann schon. Man muss sich nicht mehr kümmern und „es machen ja eh alle".

Notetaker sind toll, oder?

Es ist verständlich, dass „Notetaker" in Videokonferenzen sehr beliebt sind. Ja, Protokolle zu erstellen ist lästig. Und wer das schon häufig gemacht hat, weiß, wie mühsam und zeitaufwendig es ist. Da ist eine KI (künstliche Intelligenz), die automatisch Protokolle und Zusammenfassungen erstellt, eine wunderbare Lösung. Aber Vorsicht, es liegen einige Stolperfallen auf dem Weg!

Tools prüfen

Es ist eine gute Idee, schon vor dem Einsatz die Datenschutzbrille aufzusetzen und zu prüfen, welches Tool in der Videokonferenzlösung schon integriert ist oder Verwendung finden soll. Mitarbeitende sind aber schon mal schneller als die Brille des oder der Datenschutzbeauftragten (DSB). Deshalb ist es hilfreich, das Team zu sensibilisieren und auf mögliche Risiken und Fettnäpfchen hinzuweisen. In der heilen Datenschutzwelt sollten DSB den berühmten Senf dazugegeben haben – Daumen hoch oder Daumen runter.

Somit ist es empfehlenswert, das Thema in die regelmäßigen Schulungen einzubauen. Ratsam ist auch der Hinweis, dass Software vor dem Einsatz erst die Schleife über DSB, Geschäftsleitung und gegebenenfalls auch IT-Abteilung zu laufen hat.

Drittlandtransfer

Kommt Software aus einem Drittland zum Einsatz, dann haben wir die bekannte Zwei-Stufen-Prüfung im Gepäck.

Die erste Ebene: die Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO (Datenschutz-Grundverordnung). Hier dürfte am ehesten die Einwilligung in Betracht kommen. Das bedeutet, dass alle Beteiligten der Videokonferenz vor (!) dem Start des „Notetakers" zu informieren sind, welches Tool Verwendung finden soll. Die Informationspflichten aus Art. 13 DSGVO lassen grüßen. Verweigert eine Person die Zustimmung, darf das Tool nicht zum Einsatz kommen.

Die zweite Ebene: die Frage nach dem Schutzniveau. Auf dieser Ebene ist zu prüfen, ob es einen Angemessenheitsbeschluss der EU-Kommission gibt oder andere geeignete Garantien vorliegen, sodass das Schutzniveau gewährleistet wird. Hier sind wir bei Standardvertragsklauseln, Transfer Impact Assessment (TIA) & Co.

Bewertung durch die Datenschutzkonferenz

Handelt es sich bei der Konstellation eines Tochterunternehmens im Europäischen Wirtschaftsraum (EWR) mit einer Drittlands-Muttergesellschaft überhaupt um einen Drittlandtransfer? Dazu hat sich die Datenschutzkonferenz (DSK) in →

einem Papier vom 31. Januar 2023 geäußert. Die DSK hat ein bestehendes Weisungsrecht für einen Zugriff auf personenbezogene Daten aus dem Drittland auf ein Tochterunternehmen im EWR als nicht ausreichend für eine Übermittlung in ein Drittland im Sinne der DSGVO angesehen.

Aber auch hier kommt es auf den Einzelfall an. Somit ist nicht empfohlen, sich entspannt mit einer Tüte Chips auf die Couch zu setzen, sondern die DSGVO-Prüfbrille aufzusetzen.

Bei meiner langjährigen Tätigkeit als DSB versuche ich das Thema Drittlandtransfer zu vermeiden, wenn es sich vermeiden lässt. Wer schon einmal eine ausführliche Prüfung inklusive TIA hinter sich gebracht hat, der kennt das Thema. Daher liegt mein Fokus zuerst auf europäischen Lösungen. Ja, man wundert sich, aber es gibt sie.

Ein Blumenstrauß an Rechtsthemen

Neben der DSGVO sind noch weitere Punkte zu berücksichtigen, z.B. das Recht am gesprochenen Wort und Bild. Dieses Recht ist im Strafgesetzbuch verankert. Es handelt sich also um ein Persönlichkeitsrecht, das ein hohes Gut ist.

Startet das Tool ohne Einwilligung aller Beteiligten, dann sind wir bei einer meldepflichtigen Datenpanne. Denn Daten sind unerlaubt an einen Dritten auf die Reise gegangen. Das ist gegebenenfalls das Bild und das gesprochene Wort in Form einer Audiodatei. Da wir uns im Zeitalter der Deepfakes befinden, kann man mit einem Bild und einer Audiospur eine Menge Unsinn anstellen.

Juristen und Behörden schauen sich auch die Themen Erforderlichkeit und Notwendigkeit an. Hier stellt sich die Frage, ob die eingesetzte Software für einen bestimmten Zweck erforderlich ist, um das Ziel zu erreichen.

Dass die Software bequem ist und Zeit spart, sind nicht unbedingt Gründe, die bei den Behörden auf offene Ohren stoßen. Somit sind starke Argumente, warum das Tool zum Einsatz kommt, eine gute Idee, ebenso technische und organisatorische Maßnahmen, um sicherzustellen, dass den personenbezogenen Daten nichts passiert.

Datenschützern ist hinreichend bekannt, dass ein Datentransfer in die USA aufgrund US-amerikanischer Gesetze wie PATRIOT Act und CLOUD Act kritisch zu bewerten ist. Wie es mit dem aktuellen EU–US Data Privacy Framework aussieht, bleibt abzuwarten und im Blick zu behalten.

Was tun, sprach Zeus

Wichtig ist die vorherige (!) Information und Einwilligung der beteiligten Personen. Das sollte bei jeder Videokonferenz erfolgen. Denn es sind gegebenenfalls andere Personen in der Konferenz als in der vorherigen. Dass die Mitschrift beim letzten Mal kein Problem war, ist kein belastbares Argument.

Wer KI-Werkzeuge nutzt, um automatisch Protokolle oder Zusammenfassungen zu erstellen, sollte auf europäische bzw. deutsche Lösungen zurückzugreifen – und nicht integrierte Drittland-Tools einsetzen, weil es einfach und bequem ist. Das erspart im Übrigen auch eine Menge Arbeit und Papierkram!

Auftragsverarbeitungs-Vertrag und Subunternehmen

Nach der Auswahl eines Werkzeugs ist ein Auftragsverarbeitungs-Vertrag (AV-Vertrag) notwendig, wenn es sich um ein eigenständiges Tool handelt.

In der Literatur sind technische und organisatorische Maßnahmen beschrieben und auch die eingesetzten Subunternehmen sind genannt. Da hat man schon mal einen guten Überblick, was mit den Daten aus der Videokonferenz passiert.

Übrigens sind Unternehmen verpflichtet, alle Subunternehmen zu kennen, also die gesamte Prozesskette. Das ist dann mal wieder das nächste Thema, das den Blutdruck in die Höhe treibt.

Europäische Alternativen

Ja, es gibt europäische Alternativen. „European Alternatives“ ist ein Projekt von Constantin Graf. Die aufgeführten Produkte und Dienstleistungen haben bestimmte Kriterien zu erfüllen, bevor sie auf der Liste erscheinen. Wer neugierig ist, hier der Link: https://ogy.de/8wj9.

Auch deutsche Werkzeuge für Meeting-Notizen sind heute auf dem Markt. Diese machen auf den ersten Blick einen guten Eindruck und lassen sich in die üblichen Videokonferenzlösungen einbinden.

Ein Kriterienkatalog, welche Funktionen für Unternehmen wichtig sind, ist bei der Suche hilfreich. Wann und wie die erfassten Daten der Videokonferenz gelöscht werden, ist immer ein gutes Kriterium.

Bitte die Sensibilisierung des Teams nicht vergessen! Um hierbei auch die „Göttin der Nachweispflicht“ zufriedenzustellen, kann ein „Blatt Papier“ die wichtigsten Punkte und das Handling mit dem ausgewählten Werkzeug zusammenfassen. Das muss keine Doktorarbeit sein. Kurz und knapp die einzelnen Themen zusammenzuschreiben, hilft schon mal.

PRAXIS-TIPP

Was tun, um KI-Mitschriften rechtskonform einzusetzen? Folgende Schritte sind zu empfehlen:

- ***EU-Werkzeuge einsetzen***
- ***das Tool prüfen***
- ***AV-Vertrag abschließen***
- ***Beteiligte informieren und deren Einwilligung einholen***
- ***das Team sensibilisieren***

Dann wünsche ich viel Spaß mit „Notetaker-Tools“. Nebenbei bemerkt: Dieser Artikel ist handgemacht, ganz ohne KI.

Bettina Sandrock ist als geschäftsführende Gesellschafterin der Alarmstufe Red GmbH überzeugte Datenschützerin mit Leidenschaft und Humor.

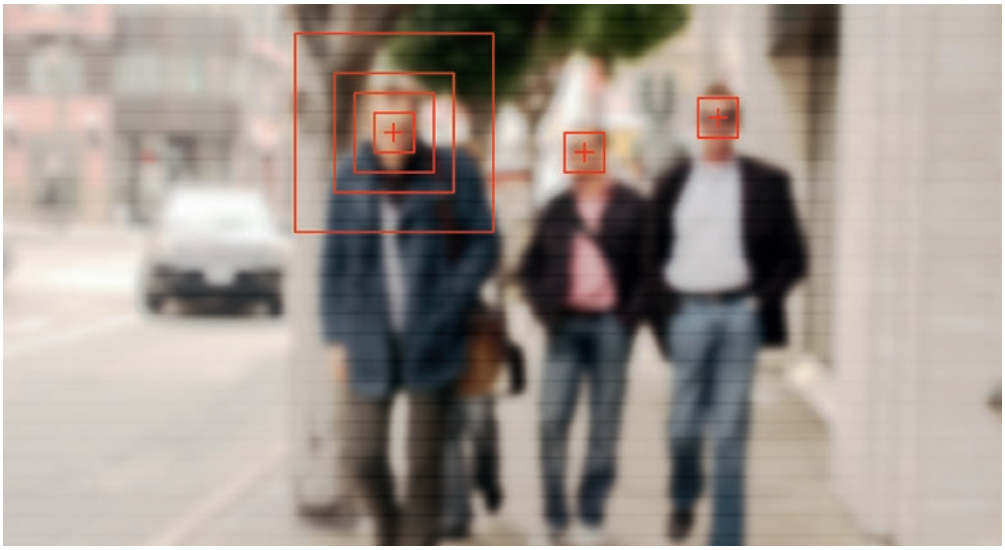


Bild: iStock.com/vasare

Es empfiehlt sich, aus den Berichten der Landesdatenschutzbeauftragten zu lernen und erforderliche Maßnahmen mittels eines strukturierten Vorgehens umzusetzen

Tätigkeitsberichte 2024

Lernen aus Datenschutzpannen

Die Tätigkeitsberichte der Aufsichtsbehörden sind für DSB sowie Unternehmen eine wichtige Informationsquelle. Sie enthalten spannende datenschutzrechtliche Fragen und Antworten aus der Praxis. Nachfolgend sind wichtige Fälle aus den 2024er-Berichten aufbereitet und mit Umsetzungsempfehlungen unterfüttert.

Videoüberwachungsmaßnahmen sind nach wie vor ein Dauerbrenner in jedem Tätigkeitsbericht. Um Bußgelder zu vermeiden, ist eine sorgsame Prüfung unerlässlich. Ein wichtiger Teilbereich der Prüfung beschäftigt sich mit der Frage nach den überwachten Bereichen und deren Sensibilität.

Dauerbrenner Videoüberwachung

Manche Bereiche sind erst auf den zweiten Blick sensibel. Dies gilt insbesondere bei neuerer Videoüberwachungstechnik mit hoher Bildauflösung oder Zoomfunktion, wie der Fall eines Hotels aus Brandenburg zeigt. Hier gab es nicht nur Kameras in den klassischen Sozialbereichen, z.B. auf Fluren vor den Hotelzimmern, in der Lobby, vor oder in den Aufzügen usw. Die Aufsichtsbehörde beanstandete eine Kamera, die das Lesegerät für Kartenzahlungen (mit-) überwachte. Denn aufgrund der hohen Auflösung waren wahrscheinlich die Eingaben der PIN etc. zu erkennen.

Bei genauerer Überlegung lassen sich weitere Bereiche identifizieren, die nur auf den ersten Blick unkritisch erscheinen, z.B.:

- Fenster, Balkone oder Terrassen benachbarter (Wohn-)Gebäude, z.B. durch Kameras auf dem Dach oder an der Fassade
- Freizeiterholungsgebiete, z.B. Parkanlagen oder Strandabschnitte
- Self-Check-in-Terminals oder Zahl-/Snackautomaten, z.B. im Hotel, Flughafen oder Kantinen und Produktionsbereichen von Unternehmen
- Räume mit Spiegelflächen (dehnen überwachte Bereiche oft unzulässigerweise aus) oder spiegelnde Glasfassaden (außen)
- Telefonkabinen in Offices oder Livestreams in Co-Working Spaces zur Auslastungsprüfung
- Gebets-/Ruheräume inkl. Zugänge, z.B. in Unternehmen oder öffentlichen Bereichen, siehe Art. 9 der Datenschutz-Grundverordnung (DSGVO)

Solchen (Teil-)Bereichen ist gemein, dass sie auf den ersten Blick verhältnismäßig harmlos wirken. Bei genauerem Hinsehen findet in diesen Bereichen allerdings oft ein Geschehen statt, das i.d.R. unbeachtet bleiben soll, insbesondere da sich aus den erhaltenen Informationen sensible Rückschlüsse auf dieses menschliche Ver- →

ONLINE-TIPP

Alle Tätigkeitsberichte der Datenschutz-Aufsichtsbehörden finden sich unter https://ogy.de/8iog.

Webcams im öffentlichen Raum

Grundsätzlich spricht bei Webcams im öffentlichen Raum nichts gegen eine gute Bildqualität. Doch neben der sorgfältigen Auswahl des Webcam-Standorts – idealerweise an einem Ort mit wenig Personenverkehr – sind besonders die erfassten Bildbereiche zu beachten. Es bietet sich an, Weitwinkelobjektive zu nutzen, Personen im Vordergrund unscharf darzustellen (Blurring) oder zu verpixeln oder solche Bereiche ganz auszuschließen. Um die Privatsphäre der Abgebildeten zu schützen, sollte zudem die Zoom- und Schwenkfunktion der Kamera deaktiviert bleiben.

Live-Stream vom FKK-Strand

In einem Fall aus Niedersachsen gab es sogar einen Livestream auf einen FKK-Strand, mit guter Auflösung, schwenkbarer Webcam und Zoomfunktion (Landesbeauftragter für den Datenschutz Niedersachsen, S. 49). FKK stand hier offensichtlich auch für „Flächendeckende Kamera-Kontrolle". Diese endete in einem Bußgeldverfahren.

halten ziehen lassen. Dass solche zunächst unscheinbar wirkenden Bereiche häufig nicht gut gekennzeichnet sind (Art. 13, Art. 14 DSGVO), erhöht die Herausforderungen in der Praxis.

ACHTUNG!

Übersichtskameras, oft in Form von Webcams, finden sich z.B. auf Golfanlagen, Campingplätzen oder bei Wetterstationen. Solche Kameras sind im Internet per Livestream abrufbar. Sie sind dafür gedacht, sich einen ersten Eindruck von der Lokalität zu verschaffen, z.B. davon, wie stark besucht der Golfplatz heute ist oder ob noch Wohnmobil-Stellplätze auf dem beliebten Campingplatz frei sind. Bei Kameras, die in der Öffentlichkeit zum Einsatz kommen, ist nicht nur auf den Datenschutz zu achten, sondern auch auf die technische Leistungsfähigkeit der Systeme und die Konfiguration – das zeigt ein Fall des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD S. 81 f.). Im beschriebenen Fall wurde dem Verantwortlichen u.a. die hohe Auflösung der Webcam zum Verhängnis: Im Vordergrund der Aufnahme waren Urlauber im Schlafanzug, quasi beim ersten Morgenkaffee, klar erkennbar.

Einwilligungen: Auf Zeitpunkt und Kontext kommt es an

Einwilligungen im Arbeitsverhältnis sind oft umstritten – insbesondere im Hinblick auf deren Freiwilligkeit im Rahmen des Über-/Unterordnungsverhältnisses. So auch in einem Fall aus Brandenburg, bei dem es um die Einwilligung zum Aushang eines Dienstplans inkl. Krankheitstagen ging.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg beanstandete unter anderem, dass die Einwilligung den Beschäftigten weder einen rechtlichen noch wirtschaftlichen Vorteil brachte (LDA Brandenburg, S. 40 ff.). Zudem verfolgten Arbeitgeber und Beschäftigte keine gleichgelagerten Interessen, denn die Organisation von Arbeitszeiten – etwa bei Schichtenübernahmen im Krankheitsfall – obliegt allein dem Arbeitgeber. Damit fehlte es an Freiwilligkeit.

Ein zentraler Kritikpunkt war der Zeitpunkt und Kontext der Einholung: Der Arbeitgeber holte die Einwilligung am ersten offiziellen Arbeitstag, dem sogenannten „Welcome Day", ein.

Beim Onboarding neuer Mitarbeiter am Welcome Day werden üblicherweise mehrere Dokumente unterschrieben oder ausgehändigt, z.B. Verschwiegenheitsverpflichtungen, Datenschutzrichtlinien und Einwilligungserklärungen für Datenverarbeitungen (z.B. Fotoveröffentlichungen auf der Unternehmenswebsite). Das dürfte bei vielen Verantwortlichen gängige Praxis sein. Hier wollen viele den Datenschutz sozusagen „mit abfrühstücken".

Jeder wird wissen, wie sich Beschäftigte dabei fühlen: schnell alles hinter sich bringen, unterschreiben, zustimmen und eben den „notwendigen Papierkram" erledigen. Und wenn ich als Beschäftigter eigentlich gar nicht in eine bestimmte Datenverarbeitung einwilligen will? Na, am Welcome Day will man ja auch nicht negativ auffallen. Dann unterschreibt man eben einfach, unabhängig davon, ob man auf die Freiwilligkeit oder die freie Widerruflichkeit im Text hingewiesen wird.

In der Praxis ist es daher essenziell, derartige Situationen zu vermeiden, um die Rechtskonformität von Einwilligungen nicht zu gefährden.

Hier bietet sich folgende Checkliste an. Unternehmen und Organisationen sollten:

1. prüfen, ob die Einwilligung im konkreten Fall tatsächlich erforderlich ist. Beispiel: Ein Unternehmen holt die Einwilligung zur Veröffentlichung von Fotos im Intranet ein, obwohl es nie Mitarbeiterfotos dort einstellt.
2. die Einwilligung in einer Situation einholen, in der nicht zu befürchten ist, Mitarbeitende zu überfordern oder zu überrumpeln, z.B. nicht unmittelbar bei Arbeitsbeginn oder parallel zu vielen anderen Dokumenten.
3. vermeiden, dass die betroffene Person durch Macht- oder Hierarchiedruck zur Einwilligung gedrängt wird, z.B. die Einwilligung nicht durch Vorgesetzte übergeben, einholen oder bei diesen abgeben lassen.
4. die Einwilligung in einem neutralen und individuellen Setting einholen, z.B. nicht in der Gruppe mit anderen neuen Mitarbeitenden.

5. die Freiwilligkeit der Einwilligung klar und verständlich kommunizieren, z.B. durch Aussagen wie: „Sie müssen das nicht unterschreiben, kein Problem."
6. den Widerruf der Einwilligung jederzeit niedrigschwellig ermöglichen und aktiv auf diese Möglichkeit hinweisen, z.B. über einfache Online-Prozesse wie das Intranet oder QR-Codes.

Je nach Ausgestaltung werden sich vielleicht nicht alle dieser Empfehlungen immer praxisgerecht umsetzen lassen. Aber schon einige dieser Empfehlungen umzusetzen, erhöht die Rechtskonformität der Einwilligung wie auch das Wohlbefinden der (neuen) Beschäftigten.

Papiermüll – der „falsche" Papierkorb im Büro?

In einer Klinik bestand die interne Regelung, Papier mit personenbezogenen Daten zunächst – vor dem Schreddern – in einem offenen Papierkorb unter dem Schreibtisch zwischenzulagern. Es kam, wie es kommen musste: Eine nicht eingeweihte Reinigungskraft entsorgte diesen Müll versehentlich in der normalen Papiermülltonne. Der Vorfall zeigt, welche Risiken vermeintlich „praktische" Umgehungslösungen bergen und vor allem, dass die Prozesse in der Praxis möglichst einfach gehalten sein sollten (ULD Schleswig-Holstein, S. 60).

WICHTIG

Der wichtigste Erfolgsfaktor für den Datenschutz insgesamt und damit auch für die rechtskonforme Datenvernichtung wird im Arbeitsalltag oft vernachlässigt: klare und vor allem schlanke, einfache Prozesse. Je komplexer ein Ablauf gestaltet ist, desto höher ist das Risiko, dass Personen ihn im stressigen Alltag vergessen, übergehen oder falsch ausführen. Datenschutz scheitert oft nicht an fehlendem Bewusstsein, sondern an unnötig komplizierten Vorgaben, die der Beschäftigte aus Bequemlichkeit oder Unaufmerksamkeit umgeht.

Deshalb gilt: Unternehmen sollten Prozesse zur Aktenvernichtung so einfach und eindeutig wie möglich gestalten – mit minimalem Interpretationsspielraum, z.B.: „Alle Ausdrucke mit personenbezogenen Daten müssen sofort nach Gebrauch in die verschlossene Datenschutztonne neben dem Drucker auf Ebene 1 eingeworfen werden!"

Daher sind auch die Platzierung und die Anzahl der Vernichtungsmöglichkeiten entscheidend. Schredder oder Datenschutztonnen müssen gut zu erreichen und unmittelbar dort verfügbar sein, wo Papiermüll anfällt, z.B. direkt neben Druckern, auf den jeweiligen Fluren, im Büro oder an Arbeitsplätzen mit viel Papierbearbeitung. Ist der Weg zur Entsorgung zu lang oder umständlich, werden Mitarbeitende ihn im Zweifel nicht gehen – z.B. wenn es nur einen Schredder pro Gebäude gibt und dieser auch noch im Keller steht.

ACHTUNG!

Externe (Reinigungs-)Dienstleister sollten nicht Teil eines „improvisierten" Entsorgungsprozesses sein, z.B. wenn Papiermüll über mehrere Stationen wandert oder zwischengelagert wird.

Es empfiehlt sich, Beschäftigte für einen klaren Vernichtungsprozess zu sensibilisieren. Dies sollte – neben Aushängen in den Arbeitsbereichen – auch Teil des Onboarding-Prozesses sein. Das Thema lässt sich z.B. sehr gut in eine Betriebsführung neuer Beschäftigter einbauen.

Ursache(n) von Schutzverletzungen als Dreh- und Angelpunkt

Datenpannen sind oft kein Zeichen schlechter Datenschutzpraxis – wenn man richtig mit ihnen umgeht. Viele Verantwortliche melden Vorfälle nach Art. 33 DSGVO – doch oft bleibt es auch intern bei der reinen Beschreibung des Problems. Eine Analyse und Ursachenforschung sind zwingend erforderlich, um Abhilfe- und Präventionsmaßnahmen umzusetzen. Doch sie fehlen häufig oder werden vernachlässigt, wie das ULD Schleswig-Holstein aufzeigt (S. 96 ff).

Die Ursachen zu analysieren, ist essenziell für Akutmaßnahmen, um Folgen einer Schutzverletzung abzumildern, wie auch für nachgelagerte Maßnahmen, um Wiederholungsfälle zu vermeiden. Nur wenn eine Organisation die Ursache ermittelt und intern aufarbeitet, →

Zwei-Stufen-Verfahren für mehr Freiwilligkeit

Ein zweistufiges Verfahren kann die Freiwilligkeit von Einwilligungen im Arbeitsverhältnis stärken. In einem ersten Schritt erhalten neue Mitarbeitende beim Onboarding lediglich Informationen über mögliche Einwilligungen sowie die Erklärungen selbst, verbunden mit dem Hinweis auf ausreichend Bedenkzeit. Erst in einem zweiten Schritt geben sie die Einwilligung tatsächlich ab. Das entkoppelt den Prozess zeitlich vom Arbeitsbeginn. Beispielsweise können Unternehmen Beschäftigte nach zwei bis vier Wochen bitten, sich mit freiwilligen Datenverarbeitungen zu befassen. Alternativ erhalten diese die Einwilligungserklärungen oder einen Link/QR-Code zur Online-Einwilligung mit dem Hinweis, dass die Abgabe freiwillig ist und sie sich dies in Ruhe anschauen können.

Bereich	Empfehlungen für ein robustes Maßnahmenmanagement
Strukturen	Klare Zuständigkeiten und Entscheidungswege festlegen – z.B. ein Datenschutzteam mit Einbindung betroffener Bereiche, um Maßnahmen schnell zu bewerten, zu koordinieren und umzusetzen, einschließlich Ursachenanalyse und Aufarbeitung
Prozesse	Einheitliche, dokumentierte Abläufe definieren, um Vorfälle zu bewerten und nachzuverfolgen – inkl. Fristen, Eskalationen, Prüfprozesse bei Systemänderungen und regelmäßiger Risikobewertung
Kultur	Offene Meldekultur fördern – z.B. keine Schuldzuweisung, stattdessen Feedbackrunden oder „Lessons-Learned"-Termine nach jedem Vorfall, inkl. aktiver Einbindung der Beschäftigten in das Maßnahmenmanagement
Dokumentation	Vorfälle und Maßnahmen strukturiert festhalten – z.B. via Standard-Template (Datum, Maßnahmen, Wirkung und Bewertung), um sie intern auszuwerten und nachzuverfolgen, wiederkehrende Muster zu identifizieren und langfristige Maßnahmen abzuleiten

Die vier Hauptbereiche für ein robustes Maßnahmenmanagement

kann sie akute Schutzverletzungen abmildern und sich zukünftige ersparen.

So ist es für die Frage nach den zu ergreifenden Maßnahmen beispielsweise wichtig zu wissen, ob der Versand einer E-Mail mit falschem Anhang (z.B. einer Rechnung) an einen Empfänger auf menschliches Versagen zurückzuführen ist oder aber auf ein systemseitiges Problem – etwa durch fehlerhafte Datenübermittlung zwischen zwei Systemen, also einen automatisierten Prozess- oder Importfehler. Eine Schutzverletzung zieht folglich je nach Ursache oft ganz unterschiedliche Maßnahmen nach sich.

In der Praxis bietet es sich daher an, eine Tabelle mit den häufigsten Ursachen von Schutzverletzungen und Maßnahmen inkl. entsprechender Zuordnung zu erstellen. Dies schafft eine Blaupause und Orientierung im Ernstfall. Dabei sind stets Abweichungen im Sachverhalt angemessen zu berücksichtigen. Es darf keinen „Ursache-/Maßnahmen-Automatismus" geben.

In einer solchen Tabelle ist jeder Ursache mindestens eine korrespondierende Maßnahme zugeordnet, einschließlich betrieblicher Umsetzungsplanung mit Zeithorizont, personellen Zuständigkeiten und Einbindung des Datenschutzbeauftragten (DSB). Zudem enthält sie Angaben zur Kontrolle und Überwachung der Maßnahmen, sowohl unverzüglicher als auch perspektivischer.

Ein kontinuierlicher Verbesserungsprozess (KVP) bei Schutzverletzungen ist nicht nur in den Grundsätzen der DSGVO angelegt (Art. 5 DSGVO), sondern auch in Art. 32 und Art. 33 DSGVO. Unterstrichen wird dies durch die Dokumentationspflicht (Art. 33 Abs. 5 DSGVO). Danach sind alle Schutzverletzungen unabhängig von ihrem Risiko entsprechend zu untersuchen und zu dokumentieren, inkl. ergriffener Maßnahmen.

WICHTIG

Laut ULD machen folgende Aspekte eine gute Meldung an die Aufsichtsbehörde aus, trotz oft unklarer Faktenlage: Die zuständige Person ergänzt die Meldung bei relevanten Neuigkeiten eigenständig (Folgemeldung); die Meldung ist sauber dokumentiert; und sie zeigt einen erkennbaren Lernprozess (Maßnahmenmanagement, kontinuierlicher Verbesserungsprozess).

Vier Hauptbereiche sind für ein robustes Maßnahmenmanagement bei Schutzverletzungen zentral. Die Tabelle oben führt sie auf.

Fazit

Es lohnt sich in jedem Fall, die Tätigkeitsberichte zu studieren und daraus Handlungsempfehlungen sowie Verbesserungsvorschläge für die eigenen Prozesse abzuleiten. Allerdings enthalten die Tätigkeitsberichte häufig nicht alle erforderlichen Schlüsse und konkreten Handlungsempfehlungen. Diese herauszuarbeiten und für das Unternehmen passgenau zu formulieren, ist eine der Kernaufgaben von DSB.

ONLINE-TIPP

Die Aufsichtsbehörde Sachsen-Anhalt hat eine sehr anschauliche Tabelle für die häufigsten Ursachen von Schutzverletzungen erstellt. Diese kann als Fundament für die eigene Tabelle dienen, abrufbar unter: https://ogy.de/oaqn.

Dr. Kevin Marschall, LL.M. ist Geschäftsführer der GDPC GbR, einer auf Datenschutz spezialisierten Unternehmensberatung mit Sitz in Kassel. Er ist primär als externer DSB tätig und befasst sich täglich mit den Herausforderungen der DSB-Tätigkeit in unterschiedlichsten Organisationen.

Nützliches Symbol („Icon“)

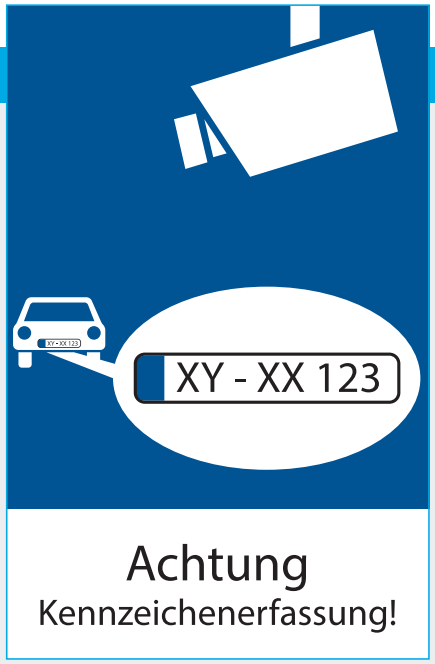
Kennzeichenerfassung

In öffentlichen Parkhäusern, aber auch auf Firmenparkplätzen setzt sich die automatische Kennzeichenerfassung immer mehr durch. Schon wegen der Informationspflichten aus Art. 13 DSGVO ist es geboten, bereits bei der Einfahrt in das Parkgelände auf die Erfassung der Kennzeichendaten hinzuweisen. Denn jedenfalls bei Fahrzeugen von Privatpersonen sind diese Daten personenbezogen.

Bisher gab es allerdings weder ein offizielles noch ein allgemein übliches Symbol, das Parkplatzsuchenden eine rasche erste Orientierung bieten kann. Diese Lücke schließt nunmehr ein Symbol zur Kennzeichenerfassung, das auf eine Initiative des Arbeitskreises Videoüberwachung der Datenschutzkonferenz (DSK) zurückgeht.

Das Symbol ist frei verwendbar

Dieses Symbol kann gratis heruntergeladen und frei verwendet werden. Wichtig dabei: Die Verwendung dieses Symbols entbindet nicht von der Pflicht, sämtliche durch Art. 13 DSGVO gebotenen Informationen zur Verfügung zu stellen, etwa in Form eines Aushangs. Ferner muss zusätzlich eine Rechtsgrundlage für die Erfassung der Kennzeichendaten vorhanden sein, etwa in Form eines „Parkvertrags“ (= Mietvertrag über die Nutzung der Parkfläche). Das Symbol stellt kein Verkehrszeichen im Sinne der Straßenverkehrsordnung dar.



Das Symbol steht als PDF-Dokument beispielsweise bei der Datenschutzaufsicht Baden-Württemberg zur Verfügung, siehe https://ogy.de/g28l.
Die Datenschutzaufsicht Hamburg bietet unter https://ogy.de/hxpk ergänzend außerdem ein als „Begleittext“ bezeichnetes Informationsblatt zum Symbol an.

Bild: https://www.baden-wuerttemberg.datenschutz.de/symbol-kennzeichenerfassung/

Nicht in Callcentern!

Software zur Emotionserkennung

Emotionserkennungs-Software, die Wut und Ärger, aber auch Freundlichkeit erkennt, hat in Call-Centern nach Auffassung der Datenschutzaufsicht Nordrhein-Westfalen „nichts zu suchen“. Ihr Einsatz greife in unzulässiger Weise massiv in die Persönlichkeitsrechte der an einem Telefonat Beteiligten ein.

Ein Unternehmen betreibt ein Call-Center, in dem es für andere Unternehmen Kundenbeschwerden bearbeiten lässt. Dabei setzte es seit einiger Zeit ein KI-System (künstliche Intelligenz) ein, das in Echtzeit die Stimmen der Anruferinnen und Anrufer wie auch der im Callcenter beschäftigten Personen analysierte.

Insgesamt überprüfte das System mehr als 6.000 Parameter wie Sprachmelodie, Rhythmus und Stimmklang, um daraus Emotionen der an einem Telefonat beteiligten Personen zu erschließen.

Da es sich bei Stimme und Sprache von Menschen um personenbezogene Daten handelt, ist die DSGVO auf derartige Emotionsanalysen anwendbar. Eine Rechtsgrundlage für die Verarbeitung der Daten ist jedoch nicht zu erkennen.

Beschäftigte schulden keine „guten Emotionen“

Was die Beschäftigten angeht, dient die Verarbeitung von Emotionsdaten nicht zur ordnungsgemäßen Erfüllung ihrer Arbeitsverträge. Zwar stellt ein korrektes Verhalten gegenüber Anruferinnen und Anrufern für Beschäftigte einen Teil ihrer Arbeitspflicht dar. „Die geschuldete Arbeitsleistung besteht aber nicht darin, bei der Arbeit eine bestimmte emotionale Stimmung zu haben“, was „dementsprechend auch nicht überwacht werden darf“, so die Datenschutzaufsicht.

Ob die Beschäftigten in eine solche Auswertung hätten einwilligen können, musste die Datenschutzaufsicht nicht entscheiden. Denn solche Einwilligungen hatte das Unternehmen nicht eingeholt. Ob dieser Weg aus ihrer Sicht gangbar wäre, darf man bezweifeln, da sie jedenfalls einen „massiven Eingriff in die Persönlichkeitsrechte“ sieht.

Wer anruft, muss informiert werden

Gegenüber den Anruferinnen und Anrufern kann sich das Unternehmen laut Datenschutzaufsicht nicht auf ein „überwiegendes berechtigtes Interesse“ (Art. 6 Abs.1 Unterabs. 1 Buchst. f DSGVO) an der Auswertung berufen.

Da das Unternehmen die Anruferinnen und Anrufer erst gar nicht darüber unterrichtet hat, dass eine Stimmenauswertung erfolgt, wäre eine Berufung auf ein berechtigtes Interesse jedoch ohnehin schon deshalb ausgeschlossen (siehe EuGH, Urteil v. 04.07.2023 – C-252/21 – „Bundeskartellamt“, Rn 126).

Quelle: Datenschutzaufsicht Nordrhein-Westfalen, Tätigkeitsbericht 2024, S. 36-39. Der Bericht ist abrufbar unter https://ogy.de/cg8l.

Dr. Eugen Ehmann ist seit vielen Jahren umfassend aktiv als Autor, Referent und Moderator für Datenschutz in Behörden und Unternehmen.

Bild: iStock.com/metamorworks

Angesichts des aktuellen Hypes um künstliche Intelligenz werben viele Anbieter mit dem Label „KI" – teils zu Unrecht („AI-Washing"). Doch auch solche Produkte können für DSB Mehraufwand bedeuten.

AI-Washing erkennen und KI-Funktionen richtig einordnen

Wann ist „KI" wirklich KI?

Die Einführung von Tools, die mit KI-Funktionen werben, erzeugt in der Praxis teils erhebliche Aufwände. Denn Prüfprozesse sind oft noch nicht etabliert. Zur gezielten und effizienten Gestaltung von Prüfungen ist es daher umso wichtiger, zunächst zu klären, ob es sich tatsächlich um künstliche Intelligenz handelt.

AI-powered (Artificial Intelligence), KI-basiert (künstliche Intelligenz), oder Deep Learning – KI gewinnt immer mehr an Bedeutung. In dieser Zeit ist der verantwortungsvolle Umgang von Unternehmen und sonstigen Organisationen mit personenbezogenen Daten unerlässlich.

Neben anderen vergleichbaren Rahmenwerken hat auch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) kürzlich einen Fragenkatalog veröffentlicht. Dieser enthält anhand diverser Fragestellungen einen Leitfaden zur datenschutzrechtlichen Einordnung, zu Risiken sowie zu potenziellen Abhilfemaßnahmen (siehe: https://ogy.de/n962).

KI-Einsatz bedeutet immer Zusatzaufwand für DSB

Solche Dokumente können in der Praxis für Datenschutzbeauftragte (DSB) absolut hilfreich sein, um die rechtlichen Rahmenbedingungen greifbarer zu machen. Dennoch entstehen ohne jeden Zweifel zusätzliche Aufwände, um sich damit auseinanderzusetzen, Prüfprozesse zu etablieren oder anzupassen und sich dann im Einzelnen mit den Tools nochmals intensiver zu befassen. Eine Frage bleibt dabei: Ist dieser Aufwand wirklich in jedem Fall notwendig?

Bevor umfangreiche Prüfprozesse überhaupt zur Anwendung kommen, stehen DSB vor einer Herausforderung: einzuordnen, ob es sich bei der zugrunde liegenden Technologie tatsächlich um KI handelt.

Denn einerseits verändern die Möglichkeiten dieser Technologien unbestritten den Arbeitsalltag und Geschäftsprozesse an vielen Stellen. Andererseits etabliert sich auch ein neues Marketingphänomen: das „AI-Washing".

Gemeint ist die Tendenz, Software oder Produkte mit dem Etikett „KI" zu versehen – selbst dann, wenn gar keine oder aber nur sehr einfache automatisierte Prozesse im Hintergrund wirken. Ziel ist es dabei oft, Aufmerksamkeit zu erzeugen, Investoren zu beeindrucken oder Kundschaft zu gewinnen.

Doch was auf den ersten Blick nach technologischem Fortschritt aussieht, stellt sich oft als Verpackung ohne substanziellen Inhalt heraus.

ACHTUNG!

Das sogenannte „AI-Washing" verleiht Softwareprodukten KI-Attribute, obwohl keine echte KI-Technologie dahintersteckt. Einige Anbieter versehen selbst unveränderte Funktionen bestehender Anwendungen plötzlich mit KI-Etiketten. Prüfen Sie daher zunächst sorgfältig, ob tatsächlich KI zum Einsatz kommt, bevor Sie weiterführende Maßnahmen einleiten oder Entscheidungen auf unbestätigte Annahmen stützen.

Was versteht man unter KI?

Seit ihrer Entstehung in den 1950er-Jahren ist die künstliche Intelligenz Gegenstand intensiver Forschung und Diskussion. Eine feste Definition hat sich bis heute nicht durchgesetzt. Vielmehr handelt es sich bei KI um ein Forschungsgebiet, das

sich stetig weiterentwickelt. Dieses zielt darauf ab, menschliches Denkvermögen in technischen Systemen algorithmisch umzusetzen, sodass diese eigenständig und anpassungsfähig agieren können.

KI-Systeme im Sinne der EU-Gesetzgebung

Die KI-Verordnung der Europäischen Union (AI Act) definiert ein „KI-System" als ein maschinengestütztes System, das in der Lage ist, in einem bestimmten Umfang autonom zu agieren. Das bedeutet, es kann Aufgaben selbstständig ausführen, ohne bei jedem Schritt direkte menschliche Steuerung zu benötigen.

Dabei ist es nicht erforderlich, dass das System vollständig unabhängig arbeitet. Denn auch eine teilweise Automatisierung fällt bereits unter diese Definition. Folgende Punkte sind von Bedeutung:

- Die KI-Verordnung hebt hervor, dass KI-Systeme nach ihrer Inbetriebnahme lern- und anpassungsfähig sind. Sie entwickeln ihre Funktionsweise kontinuierlich weiter, indem sie neue Muster erkennen oder Erfahrungen integrieren.
- Wesentliches Merkmal ist außerdem die Verarbeitung von Eingabedaten: KI-Systeme nehmen Informationen aus ihrer Umgebung oder digitalen Quellen auf und nutzen diese, um bestimmte Ziele zu verfolgen. Diese Ziele können ausdrücklich vorgegeben sein (explizite Ziele). Sie können sich aber auch aus dem Gesamtkontext ergeben (implizite Ziele).
- Das System erzeugt auf dieser Basis konkrete Ergebnisse, die in unterschiedlicher Form auftreten können: etwa als Vorhersagen, generierte Inhalte, Empfehlungen oder automatisierte Entscheidungen. Diese Ausgaben haben das Potenzial, reale (physische) oder digitale (virtuelle) Umgebungen zu beeinflussen – beispielsweise durch die Steuerung von Maschinen, durch Eingriffe in Nutzerinteraktionen oder durch automatisierte Prozesse in Softwareanwendungen.

Technische Merkmale eines KI-Systems

Aus technischer Sicht zeichnet sich künstliche Intelligenz vorrangig dadurch aus, komplexe Denkprozesse mithilfe von Algorithmen und großen Datenmengen nachzubilden, eigenständig Muster zu erkennen und daraus Entscheidungen abzuleiten.

Die wichtigsten Technologien sind die folgenden:

- Maschinelles Lernen (ML): ein KI-Teilgebiet, bei dem Algorithmen aus Daten selbstständig lernen. Sie analysieren Muster, bilden daraus Modelle und wenden diese zur Prognose oder Klassifikation neuer Daten an.
- Neuronale Netze: von biologischen Neuronen (Nervenzellen) inspirierte Algorithmen, die komplexe Muster verarbeiten. Sie bestehen aus vernetzten künstlichen Neuronen, die Informationen schichtweise abstrahieren.
- Deep Learning: Ein spezieller Bereich von ML mit tiefen neuronalen Netzen aus vielen Schichten und Parametern. Mithilfe leistungsstarker Hardware lernen diese Netze, eigenständig komplexe Aufgaben zu lösen.
- Natural Language Processing (NLP): Methoden zur automatisierten Verarbeitung natürlicher Sprache. Große Sprachmodelle (Large Language Models, LLMs) erkennen Zusammenhänge, interpretieren Kontexte und erzeugen menschenähnliche Texte für Anwendungen wie Chatbots oder auch Übersetzungen.

Beispiele: Wenn KI draufsteht, aber nicht drinsteckt

Die zuvor beschriebenen technischen Merkmale echter künstlicher Intelligenz fehlen bei genauerer Betrachtung bei zahlreichen Systemen, obwohl deren Anbieter sie als „KI" vermarkten. DSB sollten beispielsweise bei folgenden Konstellationen genau hinsehen:

- Regelbasierte Chatbots reagieren auf Schlüsselwörter nur mit fest einprogrammierten Antworten, ohne Kontextverständnis oder Lernverhalten.
- „If-then-Tools" (Wenn-dann-Werkzeuge) führen exakt vordefinierte Schritte aus, sobald eine Bedingung erfüllt ist – z.B. blockiert ein Spamfilter eingehende E-Mails, sobald er bestimmte Schlüsselwörter, verdächtige Links oder bekannte Phishing-Domains erkennt. Außerhalb der definierten Bedingungen und Regeln erfolgt hingegen keine intelligente Erkennung beispielsweise neuartiger Bedrohungen.
- Statische Empfehlungssysteme erzeugen Vorschläge allein auf Basis fester Zuordnungen aus historischen Daten, ohne sich durch neue Informationen weiterzuentwickeln – ein Beispiel: Den Kunden, die Produkt A gekauft haben, wird entsprechend einem zuvor definierten Muster Produkt B empfohlen.

PRAXIS-TIPP

- ***KI-Etikett hinterfragen: Nur weil ein Anbieter von „KI" spricht, bedeutet das nicht automatisch, dass es sich um KI handelt. Bevor eine Organisation aufwendige Compliance-Prüfungen – etwa anhand des Fragenkatalogs der BfDI – anstößt, sollte sie zunächst feststellen, ob es sich bei der eingesetzten Technologie tatsächlich um künstliche Intelligenz handelt.***
- ***Technologieneutral bewerten: Maßgeblich aus Sicht eines DSB ist nicht allein die Technik, sondern ob und wie personenbezogene Daten verarbeitet werden.***
- ***Risikoorientiert vorgehen: Die grundsätzlichen Prüf- und Dokumentationspflichten aus dem Datenschutz bleiben bestehen und richten sich u.a. nach dem Risiko. Auch einfache, regelbasierte Systeme können z.B. Datenschutz-Folgenabschätzungen erforderlich machen.***

Patrick Weber ist deutschlandweit als externer Informationssicherheits- und Datenschutzbeauftragter für die MORGENSTERN consecom GmbH tätig.

Bild: iStock.com/gorodenkoff

Der lokale Betrieb von KI-Umgebungen löst einige datenschutzrechtliche Probleme des KI-Einsatzes, aber nicht alle

Künstliche Intelligenz datenschutzkonform einsetzen

Lokale KI-Lösungen und der Datenschutz

Immer mehr Unternehmen setzen in vielen Bereichen auf künstliche Intelligenz (KI). Hinsichtlich des Datenschutzes sorgt das durchaus für Probleme. Betreibt man KI-Anwendungen lokal, sieht das zwar etwas anders aus. Aber auch hier gilt es einiges zu beachten.

Nutzen Unternehmen KI-Lösungen aus dem Internet, gelangen über kurz oder lang sensible Daten aus dem Unternehmen in die Cloud. Generative KI-Lösungen nutzen Large Language Models (LLMs). Diese müssen lernen, um richtig arbeiten zu können. Das Lernen erfolgt auch auf Basis der Daten, die Benutzer bei der Verwendung eingeben, und aus den Fragen, die Anwender stellen. Schlussendlich profitieren damit dann auch andere, dritte Nutzer der KI-Lösung von heiklen Unternehmensdaten. Das stellt ein Problem dar, nicht nur bezüglich des Datenschutzes.

Eine Alternative besteht darin, lokal KI-Server zu betreiben. In diesem Fall bleiben alle Daten im lokalen Rechenzentrum. Das ist aus Sicht des Datenschutzes sehr viel besser. Notwendig sind dazu schnelle Server, idealerweise mit Prozessoren, die KI-Lösungen unterstützen, etwa NPUs oder spezielle Hardware von NVIDIA und AMD.

KI-Server und Open Source

Die Basis vieler KI-Server ist Open Source. Betreiben lassen sich die Lösungen z.B. mit Ubuntu. Die KI selbst steht ebenfalls oft als Open-Source-Modell zur Verfügung. Ein Beispiel ist Ollama (https://ollama.com). Hier lassen sich verschiedene LLMs integrieren, auch parallel. Dazu kommen grafische Bedienoberflächen wie OpenWebUI (https://openwebui.com).

Diese beiden Anwendungen stehen als Open Source kostenlos zur Verfügung und lassen sich auf geeigneter Hardware in wenigen Minuten einrichten. Die Anwender arbeiten dann mit einem lokalen KI-Server. Alle Daten verbleiben im lokalen Netzwerk. Ollama und OpenWebUI bieten zudem eine eigene Benutzerverwaltung.

Mobile Plattformen im Fokus

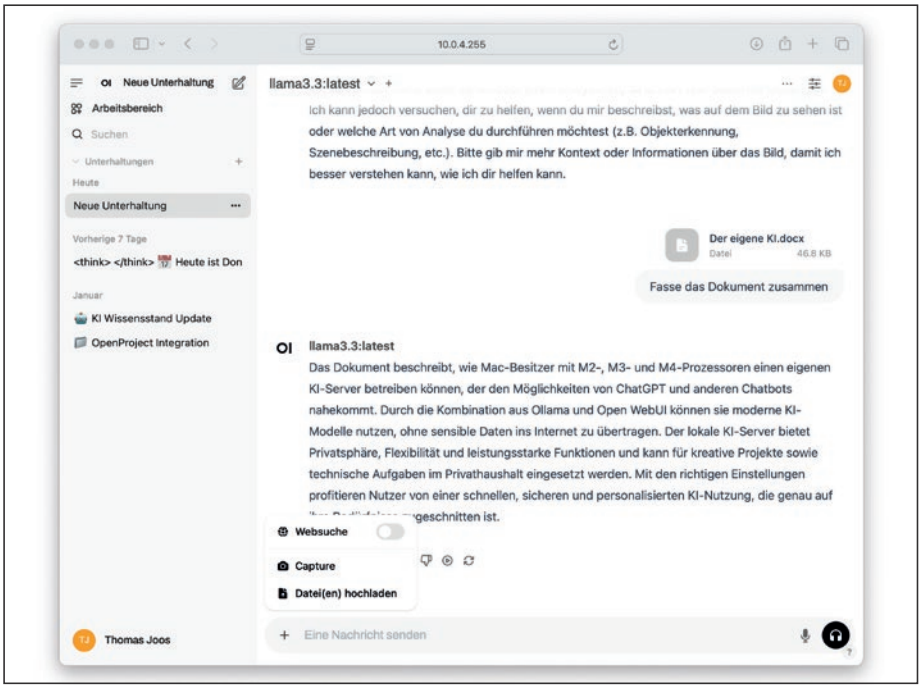
Auch mobile Plattformen geraten zunehmend ins Blickfeld. Mit der Google AI Edge Gallery steht eine quelloffene Android-App bereit, die Sprachmodelle direkt auf dem Gerät ausführt. Ohne Zugriff auf die Cloud, ohne Übermittlung sensibler Inhalte an Drittanbieter. Für Unternehmen, die Mitarbeitenden den Einsatz von KI auf mobilen Endgeräten ermöglichen wollen, markiert dies einen Wendepunkt in Sachen Datenschutz.

Das gilt allerdings nur dann, wenn Gerätekonfiguration, Datenhaltung und Zugriffskontrolle systematisch abgesichert sind. Die mitgelieferte Prompt-Engine erlaubt es, Aufgabenprofile granular anzupassen. Das engt den Rahmen für eine regelkonforme Nutzung weiter ein. Die datenschutzrechtliche Bewertung verlagert sich von der Infrastruktur zur Applikationsebene.

Technik mit rechtlichen Tücken

Ein Sonderfall sind Bibliotheken wie llama.cpp. Sie ermöglichen es, Sprachmodelle auf diversen Architekturen lokal auszuführen. Die technische Vielfalt bedeutet jedoch auch: Es gibt keine standardisierte Implementierung, keine zentrale Instanz, kein übergreifendes Rechtekonzept.

Unternehmen, die solche Frameworks einsetzen, müssen selbst für Logging, Zugriffstransparenz und eine revisionssichere Protokollierung sorgen. Andernfalls ergibt sich bei der ersten Datenschutzprüfung ein lückenhaftes Bild.



Screenshot: Thomas Joos

Ollama und OpenWebUI ermöglichen den Betrieb eines lokalen KI-Servers

Konsumentenfreundlicher, aber datenschutzrechtlich nicht minder anspruchsvoll präsentieren sich Anwendungen wie Jan AI, LM Studio oder Msty. Alle drei arbeiten lokal und umgehen damit prinzipiell das Cloudproblem. Sie eröffnen jedoch durch APIs (Schnittstellen) und externe Modellquellen neue Schwachstellen. Wo Drittanbieter Zugriff auf Modellparameter, Prompt-Daten oder Rückgabewerte erhalten, endet die Kontrolle über personenbezogene Inhalte.

ACHTUNG!

In der Praxis müssen Datenschutzbeauftragte klären, ob der Datenfluss einer KI-Software vollständig im Geltungsbereich der DSGVO (Datenschutz-Grundverordnung) verbleibt oder ob ein internationaler Drittstaatentransfer implizit stattfindet. Daraus ergeben sich Anforderungen an die Auftragsverarbeitung wie auch an die Risikobewertung der KI-Lösung.

LM Studio bietet mit der Optimierungstechnik Speculative Decoding ein Verfahren, das sensible Inhalte effizient verarbeiten kann. Deshalb gehört jede produktive Nutzung unter datenschutzrechtliche Aufsicht. Eine nachweisbare Zweckbindung, eine dokumentierte Aufbewahrungsdauer und ein generisches Löschkonzept sind zwingend erforderlich. Dabei spielt es keine Rolle, ob das Modell lokal läuft oder ob das nur scheinbar der Fall ist.

Hybride Architektur

Bei Msty ist besonders die hybride Nutzung erwähnenswert. Lokale Modelle kombiniert mit zentralen Ollama-Servern erzeugen verteilte Datenströme. Für Datenschutzverantwortliche bedeutet das eine Analysepflicht für sämtliche Stationen der Datenverarbeitung. Auch der Export von Modellen in externe Tools oder IDEs über Plugins für JetBrains oder VS Code öffnet Schnittstellen, die klar zu definieren, dokumentieren und regelmäßig zu auditieren sind.

Workspaces mit begrenzter Kontrolle

AnythingLLM bringt ein leistungsfähiges Workspace-Konzept mit, bietet aber keine granulare Rechteverwaltung. Im Unternehmenskontext bedeutet das: Jeder Zugriff auf Daten eines Workspaces gilt als potenzieller Zugriff durch sämtliche eingeloggten Benutzer. Aus datenschutzrechtlicher Sicht ist das problematisch. Auch die Vektor-Datenbanken für Embeddings sind genau zu betrachten. Ein eingebundener SaaS-Dienst bedeutet, dass die Daten das unternehmenseigene System verlassen. Faktisch handelt es sich um einen Export, der entsprechende Schutzmaßnahmen erfordert.

Begrenzte Eignung einfacher Tools

Abseits dieser vollwertigen Plattformen existieren mit GPT4All und KoboldCpp zwei Werkzeuge, die durch eine benutzerfreundliche Bedienung bestechen. Aus Sicht des Datenschutzes fehlt hier meist jede Form von Zugriffskontrolle, Logging oder Rechtekonzept. Beide Tools eignen sich allenfalls für Einzelarbeitsplätze mit klar abgegrenztem Aufgabenprofil. Für regulierte Umgebungen oder datenintensive Anwendungen bieten sie keine tragfähige Grundlage.

Fazit

Der lokale Betrieb von KI-Anwendungen schafft zweifellos datenschutzrechtliche Vorteile, löst jedoch nicht alle grundlegenden Probleme. Während der Verzicht auf cloudbasierte Modelle die Kontrolle über sensible Informationen erhöht, entstehen neue Herausforderungen auf technischer und organisatorischer Ebene. Entscheidend ist nicht allein der Ort der Verarbeitung, sondern die Qualität der Zugriffskontrollen, die Dokumentation der Datenflüsse und die Integrität der eingesetzten Komponenten.

Werkzeuge wie Ollama, AnythingLLM oder LM Studio können helfen, regulatorische Anforderungen zu erfüllen, erfordern jedoch eine sorgfältige Bewertung der gesamten Systemarchitektur. Unternehmen, die Sprachmodelle intern einsetzen wollen, benötigen klare Richtlinien, technische Schutzmaßnahmen und ein konsistentes Datenschutzkonzept. Nur so lassen sich Potenziale nutzen, ohne Haftungsrisiken einzugehen.

Thomas Joos ist IT-Experte. Darüber hinaus ist er Autor von über 100 Fachbüchern und freiberuflicher Journalist mit über 30 Jahren Erfahrung.

Bild: iStock.com/panida wijitpanya

Ein Urteil des Verwaltungsgerichts Hannover setzt Tricksereien bei der Gestaltung von Cookie-Bannern klare Grenzen. Für Website-Nutzer und den Datenschutz ist das ein Gewinn.

Rechtssichere Gestaltung minimiert Datenschutzrisiken

Cookie-Banner richtig umsetzen

Die Gestaltung von Cookie-Einwilligungsbannern auf mehreren Ebenen, verbunden mit intransparenter Nutzerführung und missverständlichen Bezeichnungen, kann die wirksame Erteilung einer Einwilligung verhindern.

Ein Urteil des Verwaltungsgerichts (VG) Hannover vom 19.03.2025 (Az: 10 A 5385/22) befasst sich ausführlich mit den Anforderungen an Cookie-Einwilligungsbanner. Das Urteil ist noch nicht rechtskräftig.

Inhalt des Rechtsstreits

Ausgangspunkt war eine Anordnung des Landesbeauftragten für den Datenschutz (LfD) Niedersachsen gegenüber einem niedersächsischen Medienhaus.

Streitgegenstand: Einwilligungsbanner

Beim Aufruf der Website des Medienhauses erschien ein Einwilligungsbanner als sogenannte Cookie-Wall, sodass keine weitere Aktion des Nutzers auf der Website möglich war: „Wir wollen Ihnen das optimale Nutzererlebnis bieten". In einem Kästchen oben rechts war zum Anklicken „Akzeptieren & Schließen X" vermerkt.

Im Banner war Scrollen möglich. Dann konnte der Nutzer Hinweise auf ein Widerrufsrecht, auf die Nutzung technisch notwendiger Cookies und die Information finden, dass eine Einwilligung auch zur Verarbeitung in Drittstaaten, besonders den USA, erfolge. Darunter befand sich kräftig farbig unterlegt ein Button „Alle akzeptieren" und mit weißem Hintergrund ein Button „Einstellungen".

Klickt der Nutzer auf „Alle akzeptieren" oder „Akzeptieren & Schließen X", verschwindet das Banner. Der Klick auf „Einstellungen" öffnet eine zweite Ebene des Banners, überschrieben mit „Datenschutzmanager". Ein Drop-down-Menü listet verschiedene Cookie-Arten auf, die sich unter den ersten drei Menüpunkten an- oder abschalten lassen. Bei den Punkten „Sonderkategorien" und „Funktionen" ist keine An-/Aus-Funktion hinterlegt. Beim Ausklappen weiterer Untermenüs erscheint eine Liste von Drittdienstleistern, dargestellt als nicht abwählbar. Wiederum kräftig farbig unterlegt ist der Button „Alle akzeptieren", mit weißem Hintergrund der Button „Auswahl speichern". Klickt der Nutzer auf „Auswahl speichern", öffnet sich das Einwilligungsbanner bei jedem Aufruf der Website erneut.

Ansicht des LfD Niedersachsen

Der LfD Niedersachsen ordnete gegenüber dem Medienhaus per Bescheid an, Anforderungen an wirksame Einwilligungen nach Art. 4 Nr. 11 und Art. 7 Datenschutz-Grundverordnung (DSGVO) umzusetzen, soweit für den Einsatz von lokalen Speicherobjekten, Tracking-Techniken und Drittdiensten erforderlich. Für den Google Tag Manager sei eine wirksame Einwilligung nach § 25 Abs. 1 TTDSG (Telekommunikations-Telemedien-Datenschutzgesetz; Anordnung des LfD von 2022) und Art. 6 Abs. 1 Buchst. a DSGVO einzuholen.

Denn die von den Nutzern der Website eingeholten Einwilligungen seien unwirksam, weil es an der Informiertheit und Freiwilligkeit fehle. Zudem sei das Banner irreführend und intransparent.

Urteil des VG Hannover

Im Ergebnis hat das VG Hannover die Klage des Medienhauses als unbegründet abgewiesen. Der Bescheid des LfD Niedersachsen sei rechtmäßig und das Medienhaus nicht in seinen Rechten verletzt.

Die Begründung: Es liegt keine informierte, freiwillige und eindeutige Einwilligung der Nutzer vor. Deshalb verstoße die Verwendung von Cookies und anderen Technologien auf der Website gegen § 25 TTDSG und Art. 6 Abs. 1 DSGVO. Eine Ausnahme ohne Einwilligung des Nutzers nach § 25 Abs. 2 TTDSG für technisch erforderliche Cookies war für das Gericht nicht ersichtlich.

Der Verstoß gegen das Einwilligungserfordernis folge aus mehreren Aspekten im Hinblick auf die Gestaltung des Cookie-Einwilligungsbanners.

Informiertheit

Das Gericht bezweifelt die Informiertheit in Bezug auf die Einwilligung der Nutzer. Es stützt sich dabei auf die Rechtsprechung des Europäischen Gerichtshofs (EuGH C-673/17 vom 01.10.2019). Dieser verlangt, als Mindestinformationen die Funktionsdauer und die Empfänger der in den Cookies enthaltenen Informationen anzugeben. Alle Informationen der Nutzer müssen klar verständlich und detailliert genug sein, damit diese die Funktionsweise der Cookies verstehen können.

Das VG Hannover geht im vorliegenden Fall davon aus, dass Nutzer in erster Linie die Website lesen wollen, und die erste Ebene des Banners nur überfliegen. Hier fehlt jedoch ein Verweis auf die hohe Anzahl der Drittdienstleister und die Datenverarbeitung in Drittstaaten.

Checkliste zur Gestaltung von Cookie-Bannern	Ja	Nein
Begriffe klar und eindeutig?	☐	☐
Alle notwendigen Informationen zum Umfang einer Einwilligung vorhanden?	☐	☐
Hinweis auf Ablehnungsmöglichkeit vorhanden?	☐	☐
Führt farbliche Gestaltung/Unterlegung eher zur Einwilligung?	☐	☐
Wird über die Anzahl der Drittanbieter informiert?	☐	☐
Ist das Ablehnen von Cookies genau so einfach wie die Einwilligung?	☐	☐
Sind Drittanbieter abwählbar?	☐	☐
Sind Buttons zum Anklicken klar bezeichnet? Keine Kombination mit dem Schließen („X")-Button	☐	☐
Zusätzlich beachten: EDSA-Taskforce unter: https://ogy.de/cookie-banner-taskforce	☐	☐

Die Checkliste zur Gestaltung von Cookie-Bannern ist abrufbar unter https://ogy.de/hltp

Freiwilligkeit

Eine Einwilligung ist freiwillig, wenn die betroffene Person eine Wahlmöglichkeit hat, also einwilligen oder ohne Nachteile darauf verzichten kann. Der Verantwortliche muss auf die Möglichkeit hinweisen, eine Einwilligung zu verweigern.

WICHTIG

Das Gericht ist hierzu der Ansicht: Die Gestaltung der verschiedenen Ebenen des Banners soll Nutzer gezielt dazu lenken, ihre Einwilligung abzugeben, und ihr Wahlrecht beeinflussen.

Wollen Nutzer keine Einwilligung erteilen, entsteht für sie erheblicher Mehraufwand: Sie müssen auf der zweiten Ebene des Banners durch das Drop-Down-Menü scrollen, um gegebenenfalls einzelne Drittanbieter „abzuschalten" und „Auswahl speichern" auszuwählen – und dies bei jedem Aufruf der Website erneut.

Auf der ersten Banner-Ebene findet sich keinerlei Hinweis, dass man per Klick auf „Einstellungen" die Einwilligung verweigern kann. Nur beim Scrollen steht: „[E]s besteht keine Verpflichtung, der Verarbeitung Ihrer Daten zuzustimmen, um dieses Angebot zu nutzen". Daraus ergibt sich jedoch nicht, dass es auf der zweiten Ebene möglich ist, abzulehnen. Es kann laut VG aufgrund der irreführenden Gestaltung des Banners vielmehr der Eindruck entstehen, dass keine Ablehnung möglich sei.

Irreführend sei auch die Funktion des Buttons „Alle akzeptieren" auf der zweiten Ebene. Dieser dient zwar dazu, erneut eine Einwilligung in eine umfassende Speicherung von Cookies und die Verarbeitung von Daten zu erteilen, der Nutzer kann den Button jedoch auch so verstehen, dass er damit seine persönlichen Einstellungen speichert. Dies ergebe sich auch aus der Blaufärbung des Buttons.

Auch sei der Button „Akzeptieren & Schließen X" irreführend und intransparent, denn üblicherweise diene das „X" zum Schließen. Eine Einwilligung über diesen Button sei überraschend und unüblich.

Verbindliche Willensäußerung

Nach Ansicht des VG scheitert eine wirksame Einwilligung auch daran, dass keine verbindliche Willensäußerung vorliegt. Diese erfordere das persönliche Bewusstsein, etwas rechtsgeschäftlich Erhebliches zu erklären.

Der Ausschluss einer wirksamen Einwilligung gelte vor allem für Nutzer, die auf „Akzeptieren & Schließen X" klicken. Aufgrund der überraschenden Gestaltung des Banners sei nicht von einem entsprechenden Einwilligungsbewußtsein dieser Nutzer auszugehen. Vielmehr dürften diese Nutzer annehmen, durch Anklicken des „X" das Banner nur zu schließen, ohne eine Einwilligung zu erteilen.

Verpflichtung zu „Alles ablehnen"-Button?

Aus dem Urteil des VG Hannover geht nicht hervor, dass die Möglichkeit, Cookies abzulehnen, zwingend in der gleichen Art gestaltet sein muss wie eine Einwilligung. Das VG betont jedoch, dass der Nutzer durch die Gestaltung des Cookie-Banners nicht gezielt zur Einwilligung geführt und von der Ablehnung abgehalten werden darf. Das Urteil des VG Hannover ist abrufbar unter: https://ogy.de/2qao.

Andrea Gailus ist als selbstständige Rechtsanwältin mit Schwerpunkt Datenschutz und IT-Recht in eigener Kanzlei tätig.

Bild: iStock.com/da-kuk

DSB sollten sich mit der Einkaufsabteilung abstimmen, um sicherzustellen, dass die Datensicherheitsanforderungen des Unternehmens auch innerhalb der Lieferkette angemessen Beachtung finden

Datensicherheit in der Lieferkette (Teil 3)

Identitätsmanagement bei Lieferanten

Viele Datenpannen haben Sicherheitslücken in der Lieferkette als Ursache. Cyberkriminelle missbrauchen dabei insbesondere digitale Identitäten und Berechtigungen. Für den Datenschutz ist es wichtig, dass auch bei den Lieferanten das Identitätsmanagement stimmt. Datenschutzbeauftragte (DSB) sollten darüber aufklären.

Die Gefahr durch Cyberbedrohungen hängt nicht allein von der Sicherheitsstrategie eines Unternehmens ab, sondern zu einem erheblichen Teil von der Strategie der Geschäftspartner. Dies bestätigt eine Umfrage von Sophos (https://ogy.de/u768), an der leitende Mitarbeitende aus Einkauf, Geschäftsführung und IT teilnahmen.

Ohne eine sichere digitale Lieferkette ist moderner Datenschutz nicht möglich. Das zeigt auch der Data Breach Investigations Report (DBIR) 2025 von Verizon Business (https://ogy.de/470z).

Darin heißt es, dass sich die Beteiligung Dritter an Sicherheitsverletzungen auf einen Anteil von 30 % der Vorfälle verdoppelt hat. Die Risiken im Zusammenhang mit der Lieferkette und den Partner-Ökosystemen eines Unternehmens sind also nicht zu unterschätzen.

Gleichzeitig zeigt der Report: Der Missbrauch von Anmeldeinformationen gehört mit 22 % der Vorfälle zu den häufigsten anfänglichen Angriffsmethoden. Betrachtet man alle diese Entwicklungen, stellt man fest: Viele Datenpannen haben eine unsichere Lieferkette als Ursache. Dabei sind die beteiligten Lieferanten häufig Opfer von Passwortdiebstahl und Missbrauch digitaler Identitäten.

Identitäten im eigenen Unternehmen

Laut dem Analystenhaus Gartner (https://ogy.de/al6w) sollten Unternehmen die Risikobewertungen externer Partner auf der Basis klarer Standards überarbeiten. Dazu gehören die Vorgabe aktueller Cybersicherheitsstandards, Mechanismen, um diese in Verträgen durchzusetzen, sowie ein Auditprogramm, um dem Cybersicherheitsplan Geltung zu verschaffen.

Auf sichere digitale Identitäten bezogen bedeutet das: Ein Unternehmen sollte nicht nur das eigene Identity and Access Management (IAM) prüfen. Es sollte auch bei den Lieferanten auf Maßnahmen zum Schutz der Identitäten und Berechtigungen drängen und diese hinterfragen.

Vielen Branchen haben dies bereits umgesetzt. So kennt man in der Automobilbranche TISAX (Trusted Information Security Assessment Exchange) und vergleichbare

Prüffragen	Ja	Nein
Sind die Risiken für den Datenschutz bedacht, die durch unsichere Identitäten und Berechtigungen bei den Lieferanten entstehen können?	☐	☐
Steht deshalb nicht nur das eigene Identity and Access Management auf dem Prüfstand, sondern auch das bei den Lieferanten?	☐	☐
Kommt Zwei-Faktor-Authentifizierung zum Einsatz, wenn Lieferanten Fernzugriffe auf die IT-Systeme des Unternehmens erhalten sollen?	☐	☐
Sind Vorgaben zum Identitäts- und Berechtigungsmanagement rechtlich in den Lieferverträgen vereinbart, genau beschrieben und dokumentiert?	☐	☐
Kommen bei Lieferantenaudits auch Fragen zum Identitätsmanagement vor (vergleiche z.B. VDA ISA)?	☐	☐

Die Checkliste ist abrufbar unter https://ogy.de/n8jh

Standards. Der Verband der Automobilindustrie (VDA) empfiehlt den Unternehmen, die an der Wertschöpfungskette der Automobilindustrie beteiligt sind, eine Informationssicherheit auf der Grundlage des VDA ISA (Information Security Assessment) aufzubauen (https://ogy.de/vuoz).

Ausbau der TOMs mit Blick auf Identitäten

Betrachtet man den VDA-ISA-Katalog, findet man darin Folgendes zum Thema Identitätsmanagement in der Lieferkette:

- Der Zugang zu IT-Systemen soll nur sicher identifizierten, authentifizierten Benutzern möglich sein. Geeignete Verfahren stellen die Identität eines Benutzers sicher fest. Die Auswahl der Verfahren zur Benutzerauthentifizierung erfolgt auf Basis einer Risikobewertung, mögliche Angriffsszenarien sind zu berücksichtigen.
- Die eingesetzten Verfahren zur Benutzerauthentifizierung entsprechen dem aktuellen Stand der Technik. Das bedeutet mindestens starke Passwörter nach Stand der Technik und den Einsatz höherwertiger Verfahren zur Authentifizierung privilegierter Benutzerkonten wie ein Privileged Access Management und eine Zwei-Faktor-Authentifizierung.
- Abhängig von der Risikobewertung verstärken ergänzende Maßnahmen Authentifizierungsverfahren und Zugriffsschutz. Dazu zählen ein dauerhaftes Monitoring der Zugriffe auf Unregelmäßigkeiten oder eine starke Authentifizierung sowie eine automatische Abmeldung oder Sperrung bei Inaktivität.

WICHTIG

Es ist entscheidend, in den Lieferverträgen ein zuverlässiges Identitäts- und Berechtigungsmanagement bei den Lieferanten zu fordern – für Fernzugriffe durch die Lieferanten auf die Systeme des Unternehmens auch eine Zwei-Faktor-Authentifizierung (2FA).

Identitätsmanagement in den Lieferverträgen

Die Forderungen an das IAM der Lieferanten sollten den Unternehmen aus ihrem eigenen IT-Sicherheits- und Datenschutzkonzept bekannt vorkommen. Letztlich sollten die Lieferanten die gleichen hohen Anforderungen erfüllen wie man selbst.

Nur so lassen sich eine durchgehende Datensicherheit und ein umfassender Datenschutz entlang der Supply Chain erreichen. Andernfalls würden Schwachstellen in der Lieferkette zu einem Datenrisiko im eigenen Unternehmen führen. Dies belegen die anfangs erwähnten Sicherheitsberichte.

Mit solchen Forderungen ist der eigene Einkauf nicht allein, es sollte die Lieferanten demnach nicht verwundern. Die erwähnte Umfrage von Sophos zeigt, dass ein großer Teil der verantwortlichen Einkäufer, Manager und IT-Leitenden die Brisanz von Cybersicherheitsvorfällen in der Lieferkette adäquat einstuft. Man kann auch sagen, dass Cybersicherheit und Datenschutz heute Teil der Einkaufsbedingungen sind.

PRAXIS-TIPP

Datenschutzbeauftragte sollten nicht nur das interne Management der Identitäten und Berechtigungen als Teil des Datenschutzkonzepts verstehen. Dazu gehören auch die Maßnahmen der Lieferanten und Partner in der Lieferkette, um digitale Identitäten zu schützen. Lieferantenaudits und Lieferverträge sollten entsprechend Forderungen an das IAM der Lieferanten enthalten. DSB sollten dies mit dem Einkauf und der verantwortlichen Stelle besprechen. Denn Datenpannen resultieren zunehmend aus Sicherheitslücken in der Lieferkette und dort aus unsicheren digitalen Identitäten.

Oliver Schonschek, Dipl.-Phys., ist News Analyst mit Fokus auf IT-Sicherheit und Datenschutz und Co-Host von Datenschutz PRAXIS Der Podcast. Er wurde bereits mehrfach als Top 10 Global Thought Leader für Privacy, Security und Cybersecurity ausgezeichnet, zuletzt 2025.

IMPRESSUM

Verlag:
WEKA Media GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

Herausgeber:
WEKA Media GmbH & Co. KG
Gesellschafter der WEKA Media GmbH & Co. KG sind als Kommanditistin:
WEKA Business Information GmbH & Co. KG und als Komplementärin:
WEKA Media Beteiligungs-GmbH

Geschäftsführer:
Jochen Hortschansky, Kurt Skupin

Redaktion:
Ricarda Veidt, M.A. (V.i.S.d.P.)
E-Mail: ricarda.veidt@weka.de
Natalie Ziebolz
Andreas Dumont, München
Dr. Wilhelm Greiner, Mitteilerei, Kinding

Anzeigen:
Jana Popp
Telefon: 0 82 33.23-72 62
Fax: 0 82 33.23-5 72 62
E-Mail: jana.popp@weka.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben Print + Online-Zugriff 289 € (zzgl. MwSt. und Versandkosten)
12 Ausgaben als PDF im Heftarchiv + Online-Zugriff 282 € (zzgl. MwSt.)

Druck:
Burscheid Medien GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4140

ISSN:
1614-6867

Bestellung unter:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
www.datenschutz-praxis.de

Haftung:
Die WEKA Media GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Erfüllungsort und Gerichtsstand ist Kissing.
Zum Abdruck angenommene Beiträge und Abbildungen gehen im Rahmen der gesetzlichen Bestimmungen in das Veröffentlichungs- und Verbreitungsrecht des Verlags über. Für unaufgefordert eingesandte Beiträge übernehmen Verlag und Redaktion keine Gewähr. Namentlich ausgewiesene Beiträge liegen in der Verantwortlichkeit des Autors bzw. der Autorin.

Der zweifelhafte Wert von Archiven

Nichts der Archäologie überlassen – selbst löschen!

Zu den spannendsten Orten bei Begehungen gehören Archive. Die werden immer mystischer, je mehr wir digitalisieren. Früher war hier einfach die „Ablage". Heute ist es das analoge Gedächtnis vergangener Verwaltung. Oder wie eine Kollegin sagte: „Hier riecht es nach Verantwortung. Der entgeht keiner!"

Die digitale Personalakte ist eingeführt. Mit klaren Regeln, automatisierten Fristen und sogar dokumentierter Löschung. Jetzt sollte das Archiv sich doch langsam leeren. Tut es aber nicht. Im Gegenteil: Es wirkt voller denn je – auch bedeutungsvoller.

Die scheinbar plausible Erklärung: „Na ja, das mit dem Löschen betrifft die digitalen Daten. Also das, was man eh nicht greifen kann und was auch nicht wirklich etwas wert ist. Da hinten hingegen sind die wertvollen Sachen!"

Fortbildung für die Ewigkeit

Ich entdecke Unterlagen zu einer Unterweisung aus dem Jahr 2004 – mit Teilnehmerliste, Unterschriften, sogar einer Feedback-Ecke („Referent Bartruff schlecht rasiert. Raum zu kalt"). Frage: „Warum ist das noch da?" Antwort: „Was, wenn morgen die Berufsgenossenschaft kommt und behauptet, wir hätten nie geschult?" Irgendwie verständlich. Aber leider keine Rechtsgrundlage nach über 20 Jahren.

Emotionale Zettel

Papier, liebevoll aufbewahrt in Klarsichthüllen. Inhalt: Name, Geburtsdatum, Telefonnummer. Und das nicht nur einmal. Sondern gleich von allen Mitarbeitern, die seit 1997 im Unternehmen waren.

Frage: „Weshalb ist das noch hier?" Antwort: „Teilweise arbeiten die Leute noch hier, da muss man die ja vielleicht mal anrufen. Außerdem: Das sind ja nur Zettel! Das zählt doch nicht, oder?" Doch. War damals als Grundlage einer elektronischen Datei gedacht. Zählt.

Fazit der Begehungen

Der Wille zur Erinnerung ist groß – der Wille zum Löschen ... naja. Wie sagte die Kollegin beim Rausgehen: „Wenn wir alles löschen, was alt ist, wer sind wir dann noch?" Ganz klar: Ein Unternehmen mit geregelter Archivierung und funktionierendem Datenschutz.

Eberhard Häcker ist Geschäftsführer der TDSSG GmbH und seit vielen Jahren als Datenschutzberater sowie externer Datenschutzbeauftragter tätig.

In der nächsten Ausgabe

KI-Training und Datenschutz

Beim KI-Training mit personenbezogenen Daten, gilt die DSGVO – doch welche Pflichten folgen daraus konkret?

Auskunftsrecht im Beruf

Der Auskunftsanspruch ist auch im Job zentral. Das müssen DSB zu Grundlagen und der praktischen Anwendung wissen.

Kundendaten im Webshop

Kundendaten helfen, das Webshop-Angebot zu verbessern – vorausgesetzt, die Datenverarbeitung ist rechtmäßig.