www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

Rechtssicher | vollständig | dauerhaft

August 2024

Bild: iStock/Vertigo3d

Eine ausführliche Checkliste zum Umgang mit der Auskunft bei pseudonymisierten Daten finden Sie auf Seite 4 und auf datenschutz-praxis.de

Konflikt zwischen Schutz und Offenlegung

Pseudonyme Daten und das Auskunftsrecht

Wie gehen Verantwortliche mit Auskunftsansprüchen über pseudonyme Daten nach der DSGVO um? Der Artikel zeigt Stolpersteine auf und liefert praktische Empfehlungen, insbesondere für Fälle, in denen die Verantwortlichen nicht den Pseudonymisierungsschlüssel besitzen.

Betroffene Personen können gemäß Art. 15 Datenschutz-Grundverordnung (DSGVO) von Verantwortlichen Auskunft über ihre personenbezogenen Daten verlangen. Die natürliche oder juristische Person, Behörde oder Einrichtung muss sodann prüfen, ob und, wenn ja, welche personenbezogenen Daten sie über die Antragstellerin oder den Antragsteller verarbeiten.

Typischerweise verarbeiten Verantwortliche personenbezogene Daten, die sie betroffenen Personen unproblematisch zuordnen können. Unter Umständen verarbeiten sie aber auch pseudonyme Daten. Zur Erinnerung: Pseudonyme Daten sind personenbezogene Daten, die sich nur dann einer spezifischen Person zuordnen lassen, wenn man den Pseudonymisierungsschlüssel besitzt.

Naturgemäß können Verantwortliche pseudonyme Daten nicht ohne Weiteres der beantragenden Person zuordnen. Sie können somit weder bestätigen, dass sie personenbezogene Daten über diese Person verarbeiten, noch können sie diese Daten beauskunften.

Pseudonymisierung aufheben, um Auskunft zu erteilen?

Um eine Auskunft zu erteilen, müssten Verantwortliche zunächst die Pseudonymisierung aufheben. Dies können sie jedoch nur selbst tun, wenn sie auch den Pseudonymisierungsschlüssel besitzen. Es kommt aber vor, dass die betroffene Person oder eine dritte Partei den Pseudonymisierungsschlüssel besitzt. In diesen Fällen ist für Verantwortliche unklar, ob und wie sie über die pseudonymen Daten Auskunft geben sollen oder überhaupt müssen. →

Titel
01 Pseudonyme Daten und das Auskunftsrecht

Schulen & Sensibilisieren
05 Geburtsdatum als Pflichtfeld in Onlineshops: Ist das zulässig?

Best Practice
08 Microsoft Copilot aus Sicht des Datenschutzes

News & Tipps
12 Generative KI und DSGVO
12 Chat GPT Taskforce

Beraten & Überwachen
13 Das bedeutet der Grundsatz der Zweckbindung in der Praxis
15 Bessere User Experience, weniger Privatsphäre?

Beraten & Überwachen
17 Aus TTDSG wird TDDDG und aus TMG wird DDG: Und jetzt?

Daten-Schluss
20 Spitzen-Hotdogs am Donnerstag – und das Büro ist wieder voll

Editorial

Ricarda Veidt,
Chefredakteurin

Ein (aktuell zumindest noch) ungebetener Gast …

Liebe Leserin, lieber Leser! Beschleicht Sie auch zunehmend der Eindruck, dass sich Windows Copilot – mehr oder weniger ungefragt – in alles einmischt? Dass beispielsweise ein Outlook plötzlich „Hilfe" anbietet und etwa E-Mails durchforstet, ohne dass ich ihm das angeschafft hätte?

Unsere IT hat meist zentral zeitnah für Ruhe gesorgt. Und das wird auch weiterhin so gehandhabt werden, solange der Einsatz von Copilot nicht eingehend geprüft ist. Es bleibt aber das ungute Gefühl, dass sich hier ein Tool hartnäckig und mit aller Macht an allen möglichen Stellen in den Arbeitsalltag hineindrängt. Auf jeden Fall wird die Copilot-Integration sicher viele DSB in der nächsten Zeit stark beschäftigen. Einen Überblick über einige Knackpunkte lesen Sie daher im Beitrag „Microsoft Copilot aus Sicht des Datenschutzes" ab Seite 8.

Auch die News auf Seite 12 beschäftigen sich mit KI. Sie stellen das Überblickspapier des Europäischen Datenschutzbeauftragten zu KI und den Bericht des Europäischen Datenschutzausschusses zur ChatGPT-Untersuchung vor.

Herzliche Grüße
Ihre Ricarda Veidt

Wann sich Verantwortliche auf Art. 11 DSGVO berufen können

Die DSGVO enthält für diesen Fall keine klare Regelung. Grundsätzlich folgt aus Erwägungsgrund 26 Satz 2 DSGVO, dass pseudonyme Daten weiterhin als personenbezogene Daten gelten. Sie bleiben somit relevant für ein Auskunftsverlangen.

Allerdings enthält Art. 11 Abs. 2 Satz 2 DSGVO eine Ausnahme, die vereinfacht wie folgt lautet: Verarbeiten Verantwortliche personenbezogene Daten, können aber die betroffene Person nicht identifizieren, dann findet ausnahmsweise Art. 15 DSGVO keine Anwendung.

Gretchenfrage: Wer hält den Schlüssel?

Das klingt zunächst danach, als könnten sich Verantwortliche mit Blick auf pseudonyme Daten immer auf Art. 11 Abs. 2 Satz 2 DSGVO berufen und müssten über diese überhaupt nicht Auskunft geben. Richtigerweise hängt jedoch die Frage, ob Verantwortliche die betroffene Person identifizieren können, davon ab, wer den Pseudonymisierungsschlüssel besitzt. Dies deutet auch der Europäische Datenschutzausschuss in seinen Leitlinien zum Auskunftsrecht an, ohne sich direkt auf Art. 11 DSGVO zu beziehen.

Verantwortliche besitzen den Pseudonymisierungsschlüssel: Auskunft ja

Besitzen die Verantwortlichen selbst den Pseudonymisierungsschlüssel, können sie die Pseudonymisierung eigenständig aufheben. Da sie die antragstellende Person identifizieren können, müssen sie Auskunft über die pseudonymen Daten geben. Sie können sich also nicht auf die Ausnahme nach Art. 11 Abs. 2 Satz 2 DSGVO berufen.

Betroffene Person besitzt den Pseudonymisierungsschlüssel: Auskunft nein

Ist die betroffene Person im Besitz des Pseudonymisierungsschlüssels, können die Verantwortlichen die Pseudonymisierung nicht eigenständig aufheben. Sie können die antragstellende Person nicht identifizieren, müssen also keine Auskunft über die pseudonymen Daten erteilen. Vielmehr können sie sich hier auf die Ausnahme nach Art. 11 Abs. 2 Satz 2 DSGVO berufen.

EDPB, Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht (S. 24):

„Anders als anonyme Daten (die keine personenbezogenen Daten sind) sind pseudonymisierte Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, personenbezogene Daten. Daher sind pseudonymisierte Daten, die mit einer betroffenen Person in Zusammenhang gebracht werden können – z.B. wenn die betroffene Person die entsprechende Kennung zur Verfügung stellt, die ihre Identifizierung ermöglicht, oder wenn der Verantwortliche in der Lage ist, die Daten mit eigenen Mitteln mit der antragstellenden Person in Zusammenhang zu bringen – im Rahmen des Antrags zu berücksichtigen."

ACHTUNG!

Das gilt nur dann nicht, wenn die antragstellende Person den Verantwortlichen den Pseudonymisierungsschlüssel mitteilt, um ihr Auskunftsrecht geltend zu machen. Denn dadurch ermöglicht sie es den Verantwortlichen, die pseudonymen Daten korrekt zuzuordnen.

Entscheidungsmechanismus	Stärkere Gewichtung Transparenz oder Datenminimierung	Bedeutung
Opt-in	Datenminimierung	„Wir schließen Ihre pseudonymisierten Daten von Ihrem Auskunftsersuchen aus, es sei denn, Sie sagen Ja."
Opt-out	Transparenz	„Wir schließen Ihre pseudonymisierten Daten in Ihr Auskunftsersuchen ein, es sei denn, Sie sagen Nein."

Mögliche Entscheidungsmechanismen bei der Auskunft über pseudonymisierte Daten.

Dritte besitzen den Pseudonymisierungsschlüssel: Auskunft hängt von deren Rolle ab

Besitzt eine dritte Partei den Pseudonymisierungsschlüssel, hängen die Pflichten der Verantwortlichen von der Rolle des Dritten ab.

Ist der Dritte ein Auftragsverarbeiter, können die Verantwortlichen ihn regelmäßig anweisen, die Pseudonymisierung aufzuheben. Die Verantwortlichen sind damit in der Lage, die antragstellende Person zu identifizieren. Deshalb müssen sie Auskunft über die pseudonymen Daten geben und können sich nicht auf die Ausnahme nach Art. 11 Abs. 2 Satz 2 DSGVO berufen.

Ist die Drittpartei ein separater Verantwortlicher (z.B. ein Datentreuhänder), können die Verantwortlichen sie regelmäßig nicht anweisen, die Pseudonymisierung aufzuheben. Damit sind sie nicht in der Lage, die antragstellende Person zu identifizieren. Deshalb müssen sie keine Auskunft über die pseudonymen Daten geben, sondern können sich auf die Ausnahme nach Art. 11 Abs. 2 Satz 2 DSGVO berufen. In diesem Fall sollten die Verantwortlichen die beantragende Person jedoch an die andere, separate verantwortliche Stelle verweisen.

Im Besitz des Pseudonymisierungsschlüssels	Auskunft über pseudonyme Daten erteilen (ja/nein)
Verantwortliche selbst	Ja
Betroffene Person	Nein, es sei denn, die beantragende Person stellt den Pseudonymisierungsschlüssel zur Verfügung
Dritte als Auftragsverarbeiter	Ja
Dritte als separat Verantwortliche	Nein, Verweis an andere Verantwortliche

Überblick über die möglichen Konstellationen

Unbeabsichtigte Aufhebung des Pseudonyms verhindern

Darüber hinaus stehen Verantwortliche vor der Herausforderung, dass die Auskunft über pseudonyme Daten möglicherweise unbeabsichtigt und zum Nachteil der beantragenden Person ist. Die Pseudonymisierung personenbezogener Daten dient gerade dazu, die Risiken für betroffene Personen zu senken und Verantwortliche dabei zu unterstützen, ihre Datenschutzpflichten einzuhalten.

Wenn die betroffene Person nun einen Auskunftsantrag stellt, ist ihr typischerweise nicht bewusst, dass sie damit eine Aufhebung ihrer Pseudonymisierung anstößt. Dies könnte die betroffene Person eben jenen Risiken aussetzen, die die ursprüngliche Pseudonymisierung vermeiden sollte.

Auch für diesen Fall – den Konflikt zwischen Transparenz und Datenminimierung – enthält die DSGVO keine klare Regelung. Verantwortliche können diesen Konflikt jedoch durch die antragstellende Person selbst auflösen lassen. Ist die betroffene Person im Besitz des Pseudonymisierungsschlüssels, legt Art. 11 Abs. 2 Satz 2 DSGVO nahe: Die betroffene Person entscheidet darüber, ob sie ihr Auskunftsrecht in Bezug auf pseudonyme Daten ausüben möchte. In ähnlicher Weise können Verantwortliche betroffene Personen auch darüber entscheiden lassen, wenn sie als Verantwortliche oder aber Dritte als Auftragsverarbeiter den Pseudonymisierungsschlüssel besitzen.

Verantwortliche sollten eine Opt-in-Möglichkeit geben

Aber wie sollten Verantwortliche diesen Entscheidungsmechanismus gestalten? Als Auswahl per Zustimmung (Opt-in) oder per Ablehnung (Opt-out-Mechanismus)?

Im Ergebnis liegt ein Opt-in-Mechanismus mehr im Interesse der antragstellenden Person. Zur Erinnerung, es ist der Zweck der Pseudonymisierung, die Identität der betroffenen Person zu deren eigenem Schutz zu maskieren. Verantwortliche, die Auskunft erteilen, sollten daher die Pseudonymisierung nicht vorschnell, sondern nur kontrolliert aufheben – und nur dadurch, dass die antragstellende Person ihren Willen selbst kundtut.

Hierbei ist auch zu berücksichtigen, dass die Entscheidung möglicherweise rückgängig zu machen ist. Schweigt die antragstellende Person zunächst, können Verantwortliche eine ungewünschte Auf-

hebung der Pseudonymisierung nicht mehr vollständig rückgängig machen. Denn kennen die Verantwortlichen die vormals pseudonymen Daten der antragstellenden Person, lässt sich das nicht mehr umkehren.

Wurden pseudonyme Daten hingegen vorschnell von der Auskunft ausgeschlossen, lässt sich das jederzeit beheben: Die Verantwortlichen müssen die pseudonymen Daten einfach nur nachliefern. Daher gilt, dass ein Opt-in-Mechanismus mehr im Interesse der antragstellenden Person liegt. Denn beeinträchtigen Verantwortliche die Transparenz, lässt sich dieser Umstand jederzeit heilen; beeinträchtigen sie die Datenminimierung, geht das jedoch nicht.

Fazit: Auskunft ja oder nein? – es kommt darauf an

Verarbeiten Verantwortliche pseudonyme Daten, sind sie verpflichtet, diese auch zu berücksichtigen, wenn jemand Auskunft verlangt. In bestimmten Fällen können Verantwortliche die antragstellende Person in den pseudonymen Daten identifizieren, weil entweder sie selbst oder ein Auftragsverarbeiter den Pseudonymisierungsschlüssel besitzen. Dann müssen sie typischerweise Auskunft über die pseudonymen Daten geben.

In anderen Fällen dagegen besitzt die antragstellende Person oder eine andere verantwortliche Stelle den Pseudonymisierungsschlüssel. In diesen Fällen müssen Verantwortliche die pseudonymen Daten typischerweise nicht beauskunften.

In jedem Fall sollten Verantwortliche der beantragenden Person bewusst machen, dass diese mit ihrem Auskunftsantrag eine Aufhebung ihrer Pseudonymisierung anstößt. Dann sollten sie die Person bitten, aktiv zu bestätigen, dass dies auch beabsichtigt ist.

Dr. Constantin Herfurth arbeitet als Principal Associate bei der Rechtsanwaltskanzlei Eversheds Sutherland. Seine Beratungstätigkeit umfasst alle Aspekte des Datenschutzes und der Cybersicherheit.

Todo	Erledigt
1. Pseudonyme Daten identifizieren	
Pseudonyme Daten ermitteln: Prüfen Sie, ob Sie in Ihrem Unternehmen pseudonyme Daten verarbeiten.	☐
Schlüsselinhaber oder -inhaberin bestimmen: Klären Sie, wer den Pseudonymisierungsschlüssel besitzt (Ihr Unternehmen selbst, die betroffene Person, ein Dritter als Auftragsverarbeiter oder als separater Verantwortlicher).	☐
2. Auskunftspflicht bewerten	
Schlüssel im Besitz der Verantwortlichen: Wenn Ihr Unternehmen den Schlüssel besitzt, bereiten Sie sich darauf vor, die Pseudonymisierung aufzuheben und Auskunft über die relevanten Daten zu geben.	☐
Schlüssel im Besitz der antragstellenden Person: Wenn die beantragende Person den Schlüssel besitzt, informieren Sie diese darüber, dass Sie die pseudonymen Daten nur beauskunften können, wenn diese den Schlüssel bereitstellt.	☐
Schlüssel im Besitz eines Dritten	
Dritter als Auftragsverarbeiter: Wenn die Drittpartei ein Auftragsverarbeiter ist, bereiten Sie sich darauf vor, den Auftragsverarbeiter anzuweisen, die Pseudonymisierung aufzuheben und die relevanten Daten an Ihr Unternehmen zu übermitteln.	☐
Dritter als separater Verantwortlicher: Wenn die Drittpartei ein separater Verantwortlicher ist, informieren Sie die antragstellende Person darüber, dass sie ihr Auskunftsverlangen insoweit bei dieser Drittpartei geltend machen kann.	☐
3. Vermeiden, die Pseudonymisierung unbeabsichtigt aufzuheben	
Information der antragstellenden Person: Informieren Sie die beantragende Person, dass ihr Auskunftsverlangen ihre Pseudonymisierung aufheben würde, und bitten Sie sie, dies aktiv zu bestätigen.	☐
Antragstellende Person bestätigt Aufhebung der Pseudonymisierung: Stellen Sie sicher, dass Ihr Unternehmen die Pseudonymisierung aufhebt und die relevanten Daten beauskunftet.	☐
Antragsteller schweigt oder lehnt Aufhebung der Pseudonymisierung ab: Stellen Sie sicher, dass die Pseudonymisierung bestehen bleibt.	☐
4. Einhaltung dokumentieren und nachweisen	
Erstellen Sie Richtlinien und Verfahren: Formulieren Sie klare interne Richtlinien und Verfahren, wie Auskunftsanträge bezüglich pseudonymer Daten zu handhaben sind.	☐
Antragstellende Person bestätigt Aufhebung der Pseudonymisierung: Stellen Sie sicher, dass Ihr Unternehmen die Pseudonymisierung aufhebt und die relevanten Daten beauskunftet.	☐

Checkliste für Datenschutzbeauftragte zur Auskunftserteilung über pseudonyme Daten. Die Checkliste finden Sie als Download unter www.datenschutz-praxis.de/betroffenenrechte/checkliste-auskunft-pseudonyme-daten

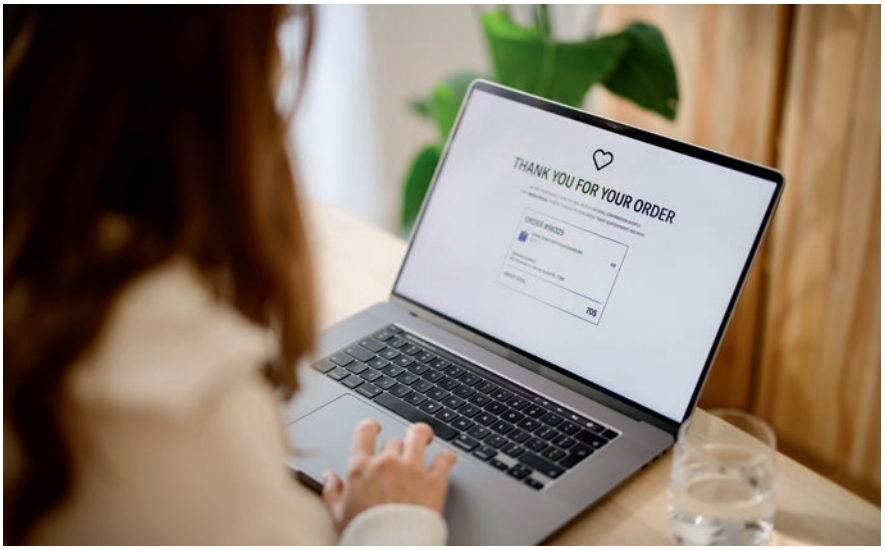


Bild: iStock/Anchiy

Das Erstellen DSGVO-konformer Formulare in Onlineshops gehört zum kleinen Einmaleins jedes Unternehmens. Nutzen Sie unsere Checkliste auch für Ihre Kollegen.

Datensparsamkeit und Rechtsgrundlage beachten

Geburtsdatum als Pflichtfeld in Onlineshops: Ist das zulässig?

Online-Bestellungen erfordern oftmals das Geburtsdatum der betroffenen Personen in Form eines Pflichtfelds. Das ist nicht immer datenschutzkonform, wie jetzt das OVG Niedersachsen entschieden hat.

Der Fall, den das Verwaltungsgericht Hannover (VG) und danach das Oberverwaltungsgericht Niedersachen (OVG) zu entscheiden hatten, betrifft eine Versandapotheke. Doch die grundsätzlichen Aussagen der Gerichte sind für alle Verantwortlichen interessant, die z.B. gegenüber Kunden mit Formularen arbeiten.

Im Rahmen des Bestellprozesses erfasst der Verantwortliche personenbezogene Daten der Kunden, darunter auch die Anrede „Herr/Frau“ und das Geburtsdatum als Pflichtfelder.

Dieser Verarbeitungsprozess unterscheidet nicht zwischen der Bestellung von Medikamenten und Drogerieartikeln. Der beschriebene Fall befasst sich ausschließlich mit dem Bestellprozess für rezeptfreie Medikamente. Bestellungen mit Rezept unterliegen einem teilweise anderen Vorgang, da der Verantwortliche das Rezept per Post erhalten muss.

Prüfverfahren der Aufsichtsbehörde

Auf die Beschwerde einer betroffenen Person hin führte die zuständige Aufsichtsbehörde, der Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen), ein Prüfverfahren nach Art. 57, 58 Datenschutz-Grundverordnung (DSGVO) durch. Der Verantwortliche verstoße gegen die Grundsätze der Rechtmäßigkeit und Datenminimierung, weil er zwingend Anrede und Geburtsdatum im Bestellprozess erhebe, so der Vorwurf.

Der Verantwortliche begründete in seiner Stellungnahme dazu die Erfassung der Anrede einerseits mit arzneimittelrechtlichen Voraussetzungen, da bestimmte Medikamente geschlechtsspezifischen Anwendungsbereichen unterlägen. Andererseits liege ein berechtigtes Interesse der Versandapotheke vor, da sie ihre Kunden und Kundinnen freundlich und angemessen ansprechen wolle. Die Verarbeitung des Geburtsdatums sei zur Erfüllung des Vertrags mit dem Kunden und aufgrund gesetzlicher Vorgaben erforderlich. Denn die Apotheke müsse überprüfen, ob Besteller volljährig seien oder der Vertrag durch Sorgeberechtigte genehmigt werden müsse. Außerdem gebe es Medikamente, die altersspezifisch zu dosieren seien. Die Apotheke sei deshalb verpflichtet, das Geburtsdatum zu verarbeiten, um nicht ihre Vertragspflichten erheblich zu verletzen.

LfD Niedersachsen untersagt Datenverarbeitung

Der LfD Niedersachsen untersagte mit Verfügung vom 08.01.2019

- die Verarbeitung des Geburtsdatums des Bestellers unabhängig von der Art des bestellten Medikaments und
- die Verarbeitung der Anrede, soweit es Medikamente betrifft, die nicht geschlechtsspezifisch zu dosieren sind.

Außerdem wies der LfD Niedersachsen den Verantwortlichen an, die Rechtsgrundlage (berechtigtes Interesse) für die Verarbeitung der Anrede im Bestellprozess in der Datenschutzerklärung aufzuführen.

Begründung: Verstoß gegen Grundsätze der DSGVO

Die Aufsichtsbehörde begründet die Verfügung mit einem Verstoß gegen den Grundsatz der Datensparsamkeit sowie gegen das Transparenzgebot. Soweit ein Medikament altersunabhängig zu dosieren sei, sei die generelle Erfassung des Geburtsdatums datenschutzrechtlich unzulässig, da dieses Datum nicht für die Erfüllung des Vertrags erforderlich sei.

Auch ein berechtigtes Interesse im Hinblick auf die Volljährigkeit des Bestellers sei nicht gegeben, denn dazu sei es ausreichend, im Bestellprozess die Volljährigkeit abzufragen. In Bezug auf die Anrede des Kunden sieht die Aufsichtsbehörde die Verarbeitung als unzulässig an, wenn es sich nicht um geschlechtsspezifische Medikamente handelt. Die fehlende Information in den Datenschutzbestimmungen zur „kundenfreundlichen Ansprache" verstoße gegen das Transparenzgebot.

Apotheke ändert Formular und Datenschutzerklärung

Die Versandapotheke ergänzte daraufhin ihr Bestellformular hinsichtlich der Anrede um die Option „ohne Angabe" und überarbeitete die Datenschutzerklärung. Diese enthält nun die Information, dass die Abfrage der Anrede zum Zweck einer freundlichen und kundenangemessenen Ansprache und Kommunikation auf Grundlage von Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO erfolgt.

In Hinblick auf die untersagte Verarbeitung des Geburtsdatums erhob die Versandapotheke Klage zum VG Hannover.

Urteil des VG Hannover: Untersagung war rechtmäßig

Das Urteil des VG Hannover (10 A 502/19 vom 09.11.2021) erklärt die Untersagungsverfügung des LfD Niedersachsen in vollem Umfang für rechtmäßig.

In seiner Urteilsbegründung befasst sich das VG sehr ausführlich mit dem Verstoß gegen das Rechtmäßigkeitsprinzip von Art. 5 Abs. 1 Buchst. a DSGVO. Ein solcher Verstoß liegt aus Sicht des Gerichts vor, weil der Verantwortliche die Verarbeitung des Geburtsdatums nicht auf eine Rechtsgrundlage von Art. 6 DSGVO stützen könne.

- Art. 6 Abs. 1 Buchst. a DSGVO entfällt, weil der Verantwortliche keine Einwilligung dafür einholt, das Geburtsdatum zu verarbeiten.
- Eine Verarbeitung des Geburtsdatums auf der Grundlage von Art. 6 Abs. 1 Buchst. b DSGVO „zur Erfüllung eines Vertrages erforderlich" liegt aus Sicht des Gerichts ebenfalls nicht vor. Denn der Verantwortliche und der Besteller schließen einen Vertrag ab, der einerseits die Übergabe der bestellten Ware und andererseits die Zahlung erfordert. Dafür ist die Verarbeitung des Geburtsdatums bei altersunabhängig zu verwendenden Produkten nicht erforderlich. Es ergibt sich auch nicht aus den speziellen Beratungs-, Informations- und Aufklärungspflichten einer Apotheke, dass solches erforderlich wäre. Denn der Bestellprozess deckt auch Drogerieprodukte und Medikamente ab, die altersunabhängig zu verwenden sind. Außerdem müsste der Verantwortliche das Alter des Anwenders und nicht des Bestellers abfragen. Darüber hinaus hält das Gericht das Argument der altersgerechten Beratung für vorgeschoben, denn sonst wären auch Fragen nach Schwangerschaft oder der Einnahme anderer Medikamente zu stellen.
- Um einen wirksam zustande gekommenen Vertrag mit einem volljährigen Besteller zu überprüfen, sieht es das Gericht – genau wie die Aufsichtsbehörde – aus Gründen der Datensparsamkeit als ausreichend an, lediglich die Volljährigkeit abzufragen.
- Die Verarbeitung des Geburtsdatums kann sich nicht auf Art. 6 Abs. 1 Buchst. c DSGVO „zur Erfüllung einer rechtlichen Verpflichtung" stützen. Der Verantwortliche argumentiert mit der Arzneimittelverschreibungsverordnung als rechtlicher Verpflichtung. Diese sieht vor, dass eine Verschreibung, also das Rezept, den Namen und das Geburtsdatum des Patienten oder der Patientin enthalten muss. Da es aber in dem Rechtsstreit ausschließlich um den Bestellprozess für nicht rezeptpflichtige Produkte geht, greift diese Rechtsgrundlage ebenfalls nicht.
- Auch die Rechtsgrundlage „berechtigte Interessen" von Art. 6 Abs. 1 Buchst. f DSGVO greift nicht. Der Verantwortliche hatte argumentiert, er müsse das Geburtsdatum erfassen, um zu wissen, ob der Besteller volljährig sei oder ob eine zusätzliche Genehmigung des Kaufvertrags durch einen Sorgeberechtigten nötig sei. Hier verweist das Gericht den Verantwortlichen auf das wesentlich mildere Mittel der einfachen Abfrage der Volljährigkeit. Deshalb fehle es bereits an der Erforderlichkeit der Verarbeitung des Geburtsdatums und eine Interessenabwägung sei nicht mehr vorzunehmen.

OVG Niedersachsen bestätigt das Urteil

Bei der Fortsetzung des Rechtsstreits vor dem OVG Niedersachsen ging es inhaltlich darum, ob die Berufung des Verantwortlichen gegen das Urteil des VG Hannover zuzulassen und damit der Rechtsstreit in der 2. Instanz nochmals zu führen war.

Der Verantwortliche stützt sich dabei im Wesentlichen auf die bereits vor dem VG Hannover vorgebrachten Argumente:

- Beratungs- und Informationspflicht der Apotheke nach Arzneimittelverordnung,
- Altersabhängigkeit der Medikamentendosierung und
- Überprüfung der Volljährigkeit.

Der Verantwortliche machte im Rahmen dieses Verfahrens zusätzlich geltend, das Geburtsdatum des Bestellers auf Basis von Art. 6 Abs. 1 Buchst. c DSGVO zu benötigen, um Personen, die ihre Betroffenenrechte z.B. auf Auskunft geltend machen, identifizieren zu können. Mit Verweis auf Erwägungsgrund Nr. 64 DSGVO lehnte das OVG dies ab. Der Verantwortliche dürfe keine Identifizierungsmerkmale aller Kunden allein zum Zweck des Identitätsnachweises bei Auskunftsersuchen verarbeiten.

Der Verantwortliche versuchte, die Verarbeitung des Geburtsdatums auf Art. 6 Abs. 1 Buchst. f DSGVO zu stützen, da das Geburtsdatum benötigt werde, um offene Forderungen gegen säumige Kunden durchsetzen zu können. Denn der Gerichtsvollzieher benötige bei der Ermittlung des Schuldners häufig das Geburtsdatum. Auch dieses Argument ließ das OVG

Prüffrage	Hinweise	Ja	Nein
Wird das Geburtsdatum zwingend abgefragt?		☐	☐
Für welchen Zweck wird das Geburtsdatum benötigt?			
Welche Rechtsgrundlage wird verwendet?			
„Zur Erfüllung eines Vertrages“ (Art. 6 Abs. 1 Buchst. b DSGVO)?	Ist das Geburtsdatum datenschutzrechtlich nicht erforderlich, ist die Verarbeitung unzulässig.	☐	☐
Zur Überprüfung der Volljährigkeit?	Geburtsdatum aus Gründen der Datensparsamkeit nicht nötig; Erfassung Volljährigkeit ja oder nein ist ausreichend	☐	☐
Rechtliche Verpflichtung (Art. 6 Abs. 1 Buchst. c DSGVO)?	Keine passende Rechtsgrundlage, wenn Geburtsdatum nur zum Zweck der Identifizierung bei der Erfüllung von Betroffenenrechten verarbeitet wird	☐	☐
Berechtigte Interessen (Art. 6 Abs. 1 Buchst. f DSGVO)?	Keine passende Rechtsgrundlage, wenn es um mögliche Forderungsausfälle geht und solche nach den Zahlungsbedingungen (z.B. Vorkasse) überhaupt nicht entstehen können. Kann im Einzelfall passende Rechtsgrundlage sein, wenn nur „auf Rechnung“ verkauft wird.	☐	☐
Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO)?	Kann passende Rechtsgrundlage sein. Eingabefelder müssen eindeutig als „freiwillig“ gekennzeichnet sein. Bestellprozess muss dann ohne Ausfüllen des Eingabefelds fortsetzbar sein. Entsprechende Informationen in der Datenschutzerklärung sind erforderlich.	☐	☐

Betreiber von Onlineshops und Datenschutzbeauftragte sollten diese Prüfung durchführen, bevor sie das komplette Geburtsdatum ihrer Kunden und Kundinnen verarbeiten. Die Checkliste ist zu finden unter www.datenschutz-praxis.de/datenschutzbeauftragte/checkliste-geburtsdatum.

ONLINE-TIPP

Das Urteil des VG Hannover lässt sich im vollen Wortlaut auf der folgenden Webseite nachlesen: https://ogy.de/590e.
Der Beschluss des OVG Niedersachsen ist hier im Wortlaut nachzulesen: https://ogy.de/45tw.

nicht gelten, da nicht dargelegt sei, welche Zahlungsmöglichkeiten der Verantwortliche anbiete. Das Risiko eines Zahlungsausfalls ergebe sich nur bei Bestellung auf Rechnung und nicht bei den anderen im Versandhandel üblichen Zahlungsbedingungen wie Vorkasse oder Kreditkarte. Aus Sicht des OVG muss der Verantwortliche eine Einwilligung des Bestellers einholen, wenn er bei Kauf auf Rechnung das Geburtsdatum verarbeiten will.

Alle anderen Argumente, die der Verantwortliche vorgebracht hatte, entschied das OVG wie bereits das VG Hannover. Im Ergebnis war die Klage auf Zulassung der Berufung am OVG erfolglos. Damit ist das Urteil des VG Hannover rechtskräftig.

Nicht nur Onlineshops betroffen

Die Überprüfung, ob die Verarbeitung bestimmter personenbezogener Daten wie des Geburtsdatums erforderlich ist, sowie die Prüfung des Verarbeitungszwecks und der Rechtsgrundlage lassen sich auf alle Verarbeitungen von Verantwortlichen übertragen.

PRAXIS-TIPP

So sollte beispielsweise auch in Bezug auf auszufüllende Formulare immer vor der Verarbeitung die Prüfung erfolgen, die die Checkliste oben zeigt. Zusammengefasst:

- Ist die Verarbeitung eines Datums wirklich notwendig?
- Zu welchem Zweck erfolgt die Verarbeitung?
- Auf welcher Rechtsgrundlage von Art. 6 DSGVO?
- Greift diese Rechtsgrundlage im konkreten Fall tatsächlich?

Fazit: Erfassung, Zweck und Rechtsgrundlage regelmäßig hinterfragen

Bei einer solchen Inventur hilft ein gut geführtes Verzeichnis der Verarbeitungstätigkeiten. Verantwortliche sollten diese Prüfungen durchführen, bevor sie Formulare und Bestellmasken in Onlineshops gestalten.

Von Zeit zu Zeit empfiehlt es sich, auch langjährig verwendete Formulare zu prüfen im Hinblick auf Erforderlichkeit der Erfassung, Zweck und Rechtsgrundlage.

Eine korrekte Beschreibung der jeweiligen Verarbeitung darf in den Datenschutzbestimmungen des Verantwortlichen ebenfalls nicht fehlen. Das minimiert Datenschutzrisiken und erspart Ärger sowohl mit Nutzern des Onlineshops als auch mit der Aufsichtsbehörde.

Rechtsanwältin Andrea Gailus ist in eigener Anwaltskanzlei tätig und befasst sich neben dem Zivilrecht schwerpunktmäßig mit IT- und Datenschutzrecht.

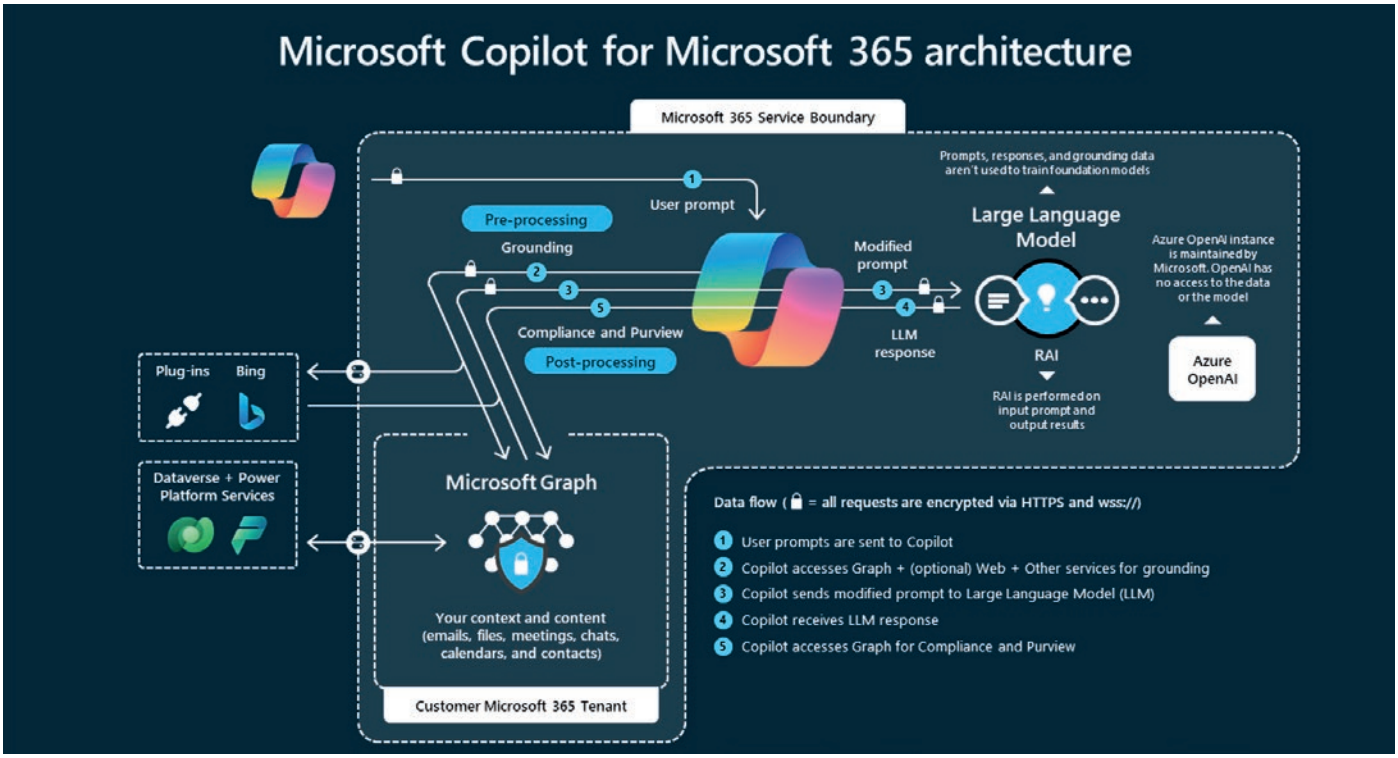


Bild: Microsoft

Nützliche Insights zur Funktionsweise des Copilot finden Sie auf https://learn.microsoft.com/de-de/copilot/microsoft-365/microsoft-365-copilot-overview

Generative künstliche Intelligenz

Microsoft Copilot aus Sicht des Datenschutzes

Der Hype um generative künstliche Intelligenz (KI) wie ChatGPT hat die Microsoft-Flaggschiffe Microsoft 365 und das Betriebssystem Windows 11 erreicht. Die KI kann vielfältige Aufgaben übernehmen und lässt sich mit natürlicher Sprache steuern. Copilot ist daher einen genaueren Blick wert.

PRAXIS-TIPP

Microsoft bietet innerhalb seiner MS-365-Umgebung ein eigenes, kostenpflichtiges Datenschutz-Tool namens „Purview". Es soll den Einsatz von Copilot überwachen, den Zugang zu sensiblen Daten feststellen und die Nutzung von KI-basierten Webdiensten abseits von Copilot wie ChatGPT regeln. Mit Datenklassifizierungen lassen sich bestimmte Daten mit einem Opt-out für Copilot versehen – inwiefern das aber auch eine Verarbeitung mit MS Graph unterbindet, zählt zu den offenen, doch dringend abzuklärenden Fragestellungen.

Die Unternehmensplattform Microsoft 365 (MS 365) ist der De-facto-Standard für cloudbasierte Office-Lösungen und gehört, wie der Name vermuten lässt, zum Konzern Microsoft. Programme wie Word, Excel, PowerPoint und Outlook lassen sich zwar auch lokal installieren. MS 365 ist in diesem Fall allerdings nur sehr reduziert als Lizenzierungsmodell zu verstehen. Die Anwendungsmöglichkeiten in der Cloud gehen weit darüber hinaus.

Plattform in der Cloud

In der Cloud können Sie mit dem Programm Teams Videokonferenzen durchführen und mit OneDrive Dateien in der Cloud ablegen und teilen. Zudem können Unternehmen eine komplette Benutzer- und Ressourcenverwaltung statt eines lokal betriebenen Domain-Controllers verwenden. Hinzu kommen die verbundenen Sicherheitslösungen in der Microsoft Cloud und die Auswertung mit Microsoft Analytics. Die Plattform setzt die Cloud-First-Strategie von Microsoft um und verarbeitet umfangreich personenbezogene Daten.

Zum Datenschutz stellten sich auch in der Vergangenheit schon viele grundsätzliche Fragen. Das betrifft etwa die Vertragsgestaltung (https://www.datenschutz-praxis.de/datenschutzbeauftragte/copilot-und-bing-chat-in-windows-11-microsoft-edge/), die Telemetriedaten bei Windows 10 (https://www.datenschutz-praxis.de/datenschutzbeauftragte/copilot-und-bing-chat-in-windows-11-microsoft-edge/) oder grundsätzlich Windows 11 (https://www.datenschutz-praxis.de/datenschutzbeauftragte/

copilot-und-bing-chat-in-windows-11-microsoft-edge/). In diese komplexe technische und regulatorische Struktur hat Microsoft mit seinem KI-Produkt „Copilot" die generative KI mit großen Sprachmodellen (Large Language Models, LLM) in die produktive Arbeitsumgebung fast aller Microsoft-Anwender eingeführt. Im Folgenden geht es darum, die datenschutzrechtlichen Fragestellungen der gewerblichen Nutzung genauer zu betrachten.

Microsoft Copilot in MS 365

Der Microsoft Copilot soll die Produkte innerhalb der MS-365-Umgebung wie Word, Excel und PowerPoint mit KI-Funktionen anreichern. Zudem ist Copilot auch als Chatbot zu nutzen, wie man es von der KI-Anwendung ChatGPT bereits kennt. Copilot lässt sich darüber hinaus mithilfe von Plug-ins erweitern. Dies ermöglicht es etwa, auf Microsofts Suchmaschine Bing zuzugreifen oder andere Datenquellen wie ein Ticketsystem für Kundenanliegen oder eine Vertriebsanwendung in Copilot einzubinden.

Mit Copilot kann man die derzeit modernste generative KI an beliebige strukturierte Unternehmensdaten anbinden, um sie dann mit natürlicher Sprache zu verwalten, auszuwerten und weiterzuverarbeiten. Im Hintergrund von Copilot werkelt das LLM GPT-4 von OpenAI. Das überrascht nicht, denn Microsoft ist der mit Abstand größte Investor bei dieser im Bereich KI führenden Tech-Firma.

Die Basis: Microsoft Graph

Wie funktioniert die Anbindung von Unternehmensdaten an die generative KI genau? Dabei spielt eine Komponente von MS 365 eine tragende Rolle, die es schon lange gibt und die mit KI nichts zu tun hat: Microsoft Graph.

Microsoft definiert es als „das Gateway zu Daten und Informationen in Microsoft 365", mit dem man „auf die enormen Datenmengen in Microsoft 365, Windows und Enterprise Mobility + Security" zugreifen kann. Dazu gehören u.a. Kalendereinträge, Excel- und Teams-Nutzung, Dateien in OneDrive, Security-Information der Microsoft-Defender-Umgebung sowie mit diesen Daten und Diensten verbundene Benutzeraktionen. Das umfasst auch die Telemetriedaten der lokal installierten Betriebssysteme Windows 10 und 11.

Sämtliche in MS 365 getätigten Aktionen und Dateninhalte landen in dieser zentralen Datenbank, die in der Microsoft Cloud gespeichert ist. Sie lassen sich über Schnittstellen abfragen. Die Graph-Datenbank stellt für sich genommen schon einige datenschutzrelevante Fragen. Das gilt insbesondere in Bezug auf die Möglichkeit, Mitarbeiterdaten mit dem MS-365-Tool Analytics auszuwerten. Dazu gesellen sich datenschutzrechtliche Verantwortlichkeiten, wenn viele eigenständige Unternehmen in einem Konzern unter einem Tenant konfiguriert sind. Diese Datenbank öffnet Microsoft nun seiner generativen KI, dem Copilot.

Anbindung an Apps, Daten und Interaktionen

Die in Microsoft Graph enthaltenen Informationen lassen sich nun mit MS-365-Apps wie Word, PowerPoint oder einer ebenfalls Copilot genannten Webanwendung verwenden. Microsoft bezeichnet diese als Apps. Es ist zudem möglich, beliebige externe Datenbanken und andere Cloud-Dienste über Konnektoren anzusteuern. Die kann man mitunter selbst programmieren. Unternehmen, die ihre Dateien in Microsofts Datenspeicher OneDrive ablegen, können auf die Inhalte dieser Dateien nun auch mit Copilot zugreifen.

WICHTIG

Mit dem Copilot steht demnach eine einfache Möglichkeit zur Verfügung, modernste KI mit eigenen Daten nutzbar zu machen, ohne sich mit KI-Programmierung oder gar dem aufwendigen Training und Finetuning eines KI-Modells abmühen zu müssen.

Windows 11 und Copilot

Wer der Meinung ist, dass eine Beschäftigung mit Copilot nur dann angeraten ist, wenn ein entsprechend lizenziertes MS-365-Produkt zum Einsatz kommt, der sollte die in Windows 11 vorgesehene Copilot-Integration nicht vergessen. In den USA gehört die KI-Funktion seit Herbst 2023 zum Umfang von Windows 11.

Hier stehen, ein Microsoft-Online-Konto vorausgesetzt, ebenfalls die Copilot-Funktionen zur Verfügung, sei es als Chatbot oder ergänzt um die Auswertung der eigenen Dateien. Ohne Online-Konto sind die Anfragen limitiert. Das beruhigt aus Datenschutzsicht aber nicht unbedingt, da eine KI-Nutzung durch eigene →

Copilot ist erst der Anfang

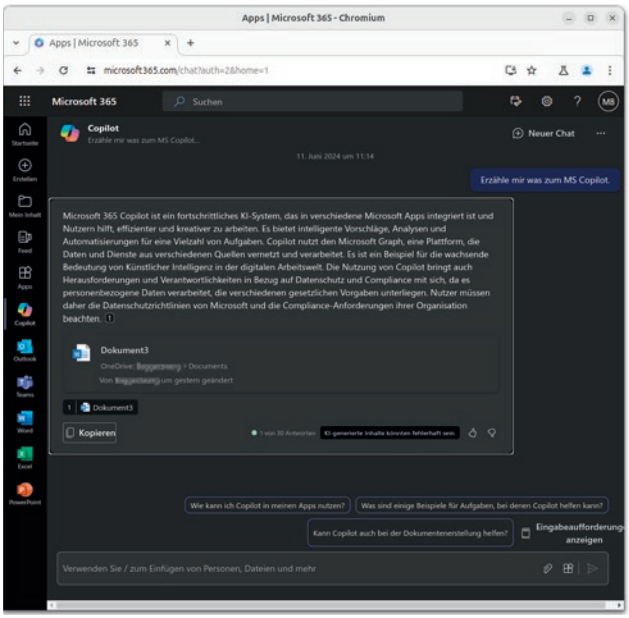
Wer meint, dass mit dem Copilot – sei es innerhalb von MS 365 oder auf einem Windows-Arbeitsplatzrechner – die Aktivitäten von Microsoft in Sachen KI erst einmal beendet sind und man sich mit der Suche nach einem datenschutzkonformen Einsatz beschäftigen kann, der irrt. Microsoft kommt mit einem neuen Produkt namens „Recall".
Recall soll sämtliche Aktivitäten auf einem Arbeitsplatzrechner samt der Anfertigung von Screenshots aufzeichnen und alles mittels KI in eine KI-basierte Suchmöglichkeit transformieren. Noch sollen die Rohdaten ausschließlich auf den Endgeräten bleiben – ob dabei auch die KI-internen Embeddings gemeint sind, bleibt zu hoffen oder bald zu überprüfen. Nach scharfer Kritik hat Microsoft den Erscheinungstermin von Recall zunächst verschoben.

WICHTIG

Im Prinzip ist Microsoft Graph der zentrale Datenspeicher eines Microsoft-Tenants. Ein Tenant ist das Haupt-Konto für Microsoft 365 und/oder Azure. Er stellt die logische Einheit dar, unter der die Benutzer, Anwendungen, Lizenzen und Daten einer Organisationseinheit zusammengefasst und verwaltet werden.

Mitarbeitende samt Weitergabe personenbezogener Daten schnell zu einem Datenschutzverstoß führen kann.

Da eine generative KI eine enorme Rechenleistung erfordert, ist eine Cloud-Anbindung in Microsoft-Rechenzentren mit dabei. Entwicklungen von speziellen KI-optimierten Windows-Clients, die den passenden Namen Copilot+ PC tragen, kommen derzeit auf den Markt. Man sollte sie in Bezug auf Datenschutz und Datenflüsse ebenfalls genau unter die Lupe nehmen.



Screenshot Andreas Sachs

Das sagt Copilot selbst zu seinen Funktionen und Herausforderungen in puncto Datenschutz

Datenschutzrechtliche Risiken

Mit Blick auf den Datenschutz kommt bei Copilot nun die Frage auf, welche besonderen Risiken beim Einsatz dieser KI-Technik auftreten können. Die von Datenschutz-Aufsichtsbehörden diskutierte Frage, ob MS 365 überhaupt datenschutzkonform sein kann, soll hier nicht im Mittelpunkt stehen, sondern der spezifische Betrieb einer künstlichen Intelligenz im Unternehmens-, aber auch im Behördenumfeld.

Microsoft Graph ist so konzipiert, dass es dem Copilot alle – auch personenbezogenen – Daten eines Tenants zur Verfügung stellt. Ein akribisch konzipiertes Rollen- und Rechtekonzept greift erst bei der Ausgabe der generativen KI – zumindest hoffentlich, da bislang keine detaillierten Informationen zum Copilot-Unterbau zur Verfügung stehen.

Das bedeutet aber auch, dass Copilot vergessene Rechtefreigaben, etwa über die Sharepoint-Plattform, schnell Mitarbeitern zur Verfügung stellen könnte, die darauf keinen Zugriff haben sollten, oder dass diese Daten gar Inhalt eines Copilot-Ergebnisses sein können.

Dies stellt mitunter eine Verletzung von Art. 33 Datenschutz-Grundverordnung (DSGVO) dar. Sie löst eine Meldepflicht bei der Datenschutzaufsichtsbehörde aus, die für den Verantwortlichen zuständig ist, der Copilot einsetzt – nicht für Microsoft.

BEISPIEL

Der niederschwellige Zugang zu hochentwickelter KI mit umfangreichen Unternehmensdaten, zu denen auch Beschäftigtendaten gehören, birgt zudem das Risiko, dass jemand Verarbeitungen „schnell mal ausprobiert". Beispiele: Die Personalerin lässt ein Bewerbungs-PDF auf die Eignung eines Bewerbers hin analysieren, oder Kollegen werten über Copilot Teams-Transkriptionen einer internen Besprechung hinsichtlich fachlicher Relevanz aus. Oder Führungskräfte nutzen Copilot, um Daten von ursprünglich zu Sicherheitszwecken erfassten Ereignissen zu verknüpfen, um herauszufinden, ob Beschäftigte im Homeoffice überhaupt arbeiten.

DSFA-Schwellenwertprüfung

Die Frage, ob eine Verarbeitung personenbezogener Daten ein voraussichtlich hohes Risiko mit sich bringt und also eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO durchzuführen ist, stellt sich auch bei Copilot.

Neben der Frage, inwiefern MS 365 samt Copilot allgemein einem hohen Risiko unterliegt, ist der jeweilige Verarbeitungszweck hierfür ausschlaggebend. Copilot an sich unterliegt keinem spezifischen Zweck, der konkrete Einsatz dagegen schon. Mit Blick auf die europäische Heuristik des Working Paper 248 (https://ogy.de/ajpc) dürfte bei Copilot der Bereich der „innovativen Technologie" erfüllt sein. Kommen

Fehlende Best Practices

Die Risiken, die sich aus der Ausgabe von generativer KI insbesondere mit Blick auf Diskriminierungen oder unrichtige Aussagen ergeben können, werden mit Copilot schon jetzt in die betriebliche Praxis gespült, bevor es einen anerkannten, wirksamen Umgang mit dieser Art von KI-Risiken gibt. Auch die Ausleitung von vertraulichen internen Daten in die Microsoft-Cloud oder gar in die Bing-Suchmaschine ist ein Problemfeld, das bei Copilot genauso wie bei ChatGPT auftreten kann – auch wenn Microsoft in seinen Vertragsbestimmungen zusagt, dass die Nutzungsdaten weder an OpenAI gehen noch als Material für das Nachtraining von zukünftigen Modellversionen dienen.

nun noch die „schutzwürdigen Betroffenen" dazu, dann ist eine DSFA-Schwelle erreicht. Dies ist etwa bei der Auswertung von Beschäftigtendaten mit Copilot immer der Fall.

Hier ist schon abzusehen, dass gerade der Beschäftigtendatenschutz einer der größten Anwendungsbereiche des Datenschutzes im Zusammenhang mit KI werden könnte.

Durchführung der DSFA

Datenschutzbeauftragte (DSB) nehmen bei einer DSFA eine zentrale Rolle ein. Daher wollte der deutsche Gesetzgeber, dass Verantwortliche bei Hochrisikoverarbeitungen immer einen oder eine DSB bestellen müssen. Dies bedeutet, dass bei Nutzung des MS Copilot mit dem Ziel, Mitarbeiterdaten zu verarbeiten – wie z.B. Bewerbungsunterlagen auszuwerten – ein DSB notwendig ist. Auch eine Transkription von Teams, die das von Teilnehmenden gesprochene Wort in Text umwandelt, dürfte darunterfallen – sofern für eine derartige Verarbeitung eine datenschutzrechtliche Grundlage existiert.

Die spezifischen KI-Risiken von generativer KI wie Diskriminierung, unrichtige Aussagen und unzulässige Verarbeitung vonseiten eines KI-Cloud-Dienstes sind in die DSFA-KI-Risikobeurteilung einzubauen. Es bestehen beim KI-Einsatz auch Compliance-Risiken dergestalt, dass KI mit Blick auf den Datenschutz nicht angemessen zum Einsatz kommt. Dies wären z.B. eine Ad-hoc-Verarbeitung ohne Eintrag ins Verarbeitungsverzeichnis, ungeprüfte Weiterverarbeitungen von Copilot-Ausgaben in geplanten Verarbeitungsprozessen und mögliche fehlende menschliche Interventionsschritte wie in Art. 22 DSGVO gefordert.

Organisatorischer Datenschutz

Art. 25 DSGVO fordert, Datenschutzrisiken mittels technischer und organisatorischer Maßnahmen einzudämmen. Bei generativer KI ist insbesondere das verwendete KI-Modell mit Blick auf dessen Trainingsdaten für verzerrende, diskriminierende oder faktisch falsche Aussagen ursächlich. Darüber ist bei Microsoft Copilot wie bei ChatGPT von OpenAI so gut wie nichts bekannt.

Deswegen ist insbesondere in der Folgeverarbeitung von Ausgaben des Copilot der angeschlossene Verarbeitungsprozess zu überwachen. Denn so gut eine generative KI auch erscheinen mag: Zu den Falschaussagen, auch „Halluzinationen" genannt, liegen wie bei anderen generativen KIs auch bei Copilot keine plausiblen Transparenzinformationen vor. So muss man im besten Fall mit einer ca. 10%igen Unrichtigkeit rechnen.

Dies lässt nur einen Schluss zu: Der Copilot kann ausschließlich dann personenbezogene Daten sinnvoll verarbeiten, wenn eine gewisse Unschärfe und Fehlerquote tolerabel sind. Beispiele sind Reden schreiben, Präsentationsentwürfe in PowerPoint erstellen oder ein Grobentwurf eines Word-Dokuments anhand eines Teams-Transkripts, wenn die Transkription an sich datenschutzkonform wäre. Eine automatisierte Auswertung von Bewerbungen mittels Copilot – ein Marketingbeispiel von Microsoft – fällt aber definitiv nicht unter diese Kategorie.

Fazit und Ausblick

Ende 2022 ist mit ChatGPT generative KI in den Fokus der Öffentlichkeit geraten. Microsoft hat die Zeichen der Zeit erkannt und ist finanzkräftig als Hauptinvestor beim Unternehmen OpenAI eingestiegen. Entsprechend hat Microsoft nicht lange gezögert, diese Technik in seine eigenen Produkte zu integrieren, sei es MS 365 oder seien es die Betriebssysteme.

Während so nun die modernste KI für all diejenigen, die die Lizenzen bezahlen, bereitsteht, sind grundlegende Fragen hinsichtlich der Regulierung noch nicht beantwortet:

- Wie geht man mit den Falschausgaben und Diskriminierungen um?
- Wie lässt sich Transparenz schaffen bei der Entscheidungsfindung?
- Wie lassen sich Betroffenenrechte wie das Löschen umsetzen?
- Und wie sieht überhaupt ein datenschutzkonformer KI-Verarbeitungsprozess aus?

Es könnte gut sein, dass die Klärung dieser datenschutzrechtlichen Grundsatzfragen nun wieder mit Blick auf Microsoft-Produkte stattfindet. Behalten Sie also den Copilot im Auge.

Andreas Sachs ist Vizepräsident des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA). Darüber hinaus leitet er das Referat Technischer Datenschutz und IT-Sicherheit beim BayLDA.

Die KI-Verordnung & die Rolle von DSB

Neben der DSGVO kommt mit der KI-Verordnung (KI-VO) ein zweites Regelwerk für die Verarbeitung personenbezogener Daten mit KI. Die KI-VO regelt primär KI-Systeme, hat aber viele Ausnahmen bei KI-Systemen mit generativer KI vorgesehen, deren wesentliches Unterscheidungskriterium der offene Verwendungszweck ist. Sollte Copilot unter diese Ausnahme fallen, dann könnte es bei Einsätzen in Bereichen, die unter die Kategorien „Hochrisiko-KI" unter der KI-VO fallen (z.B. Anwendungen mit Beschäftigtendaten), jedes Unternehmen oder jede Behörde, die Copilot einsetzt, zum KI-Anbieter werden. Sie fänden sich so in Gesellschaft von Tech-Riesen wie OpenAI und Meta, was die Anforderungen der KI-Verordnung angeht.
Da die DSGVO weiterhin gültig ist, ist es ratsam für Datenschutzbeauftragte, sich neben dem Themenfeld KI auch intensiv mit der KI-Verordnung zu beschäftigen. Die KI-VO benennt die neue Berufsrolle „KI-Beauftragter" nicht ausdrücklich. Bei Hochrisiko-KI ist sie aber von der Fachkompetenz für eine rechtskonforme Umsetzung der KI-VO erforderlich. Diese Rolle dürfte nicht im Interessenkonflikt mit den Pflichten von DSB stehen. Beratung, Schulung und Aufklärung zählen schließlich zu dessen Kernaufgaben.

Europäischer Datenschutzbeauftragter (EDSB)

Generative KI und DSGVO

Der Europäische Datenschutzbeauftragte wird künftig eine Doppelrolle haben. Schon bisher war er die Datenschutzaufsichtsbehörde für die Organe und Einrichtungen der EU (siehe Art. 52 Abs. 1 der Verordnung (EU) 2018/1725). In dieser Funktion hatte er zahlreiche Aufgaben (siehe Art. 57 der genannten Verordnung).

Zusätzliche Rolle des EDSB: „KI-Aufsichtsbehörde"

Künftig weist ihm der Artificial Intelligence Act (AI Act) außerdem die Rolle einer „KI-Aufsichtsbehörde" für die Organe und Einrichtungen der EU zu. Vor diesem Hintergrund verdienen Äußerungen von ihm zum Einsatz von KI-Anwendungen besondere Beachtung.

Darstellung zu KI in Fragen und Antworten

In einem Überblickspapier stellt er in Form von 14 Fragen und Antworten dar, welche Anforderungen sich aus den EU-Vorgaben zum Datenschutz für den Einsatz von generativen KI-Systemen ergeben. Die rechtliche Basis bilden dabei die Vorgaben der Verordnung (EU) 2018/1725, die den Datenschutz bei den Organen und Einrichtungen der EU regelt. Sie stimmen inhaltlich mit den Vorgaben der Datenschutz-Grundverordnung (DSGVO) überein.

Die Darstellung ist so aufgebaut, dass sie nach der Klärung einiger Schlüsselfragen erste Antworten gibt und einige vorläufige Schlussfolgerungen zieht. Daran schließen sich weitere Klarstellungen und Beispiele an (so Ziffer 5 der Einleitung zu dem Papier).

Zu den Schlüsselfragen gehört, was überhaupt unter generativer KI zu verstehen ist (siehe dazu Frage 1 des Papiers). Gegen den Einsatz von KI-Systemen durch EU-Institutionen ist prinzipiell nichts einzuwenden, wobei allerdings alle einschlägigen rechtlichen Vorgaben zu beachten sind, u.a. die des EU-Datenschutzrechts (so Frage 2 des Papiers).

Verarbeitung personenbezogener Daten

Zentrale Bedeutung hat die Frage, ob ein KI-System überhaupt personenbezogene Daten verarbeitet und wie sich dies feststellen lässt (Frage 3 des Papiers). Umso überraschender ist die Kürze, mit der der EDSB dies abhandelt. Angesprochen wird u.a. auch die Rolle der Datenschutzbeauftragten (Frage 4 des Papiers) und die Rolle des Prinzips der Datenminimierung (Frage 7 des Papiers). Sonst bisher eher selten diskutiert, stellt das Papier dar, ob und wann KI-Systeme automatisierte Entscheidungen im Sinn von Art. 22 DSGVO treffen (Frage 10 des Papiers).

Sehr nützlich: Zugang zu weiteren Quellen

Besonders nützlich dürfte sein, dass das Papier in der Antwort auf Frage 14 nach dem Stand vom 03. Juni 2024 wesentliche Papiere auflistet, die Datenschutzaufsichtsbehörden der Mitgliedstaaten und andere relevante Institutionen zum Thema KI bisher veröffentlicht haben. Ferner sind dort alle Dokumente verlinkt, die der EDSB selbst zum Thema KI und Datenschutz herausgegeben hat.

Quelle: European Data Protection Officer (EDPS), Generative AI and the EUDPR. First EDPS Orientations for ensuring data protection compliance when using Generative AI systems, veröffentlicht am 03. Juni 2024. Das nur in englischer Sprache verfügbare Papier hat einen Umfang von 26 Seiten. Es ist abrufbar unter https://ogy.de/n9no.

Bild: iStock/sesame

Europäischer Datenschutzausschuss (EDSA)

Chat GPT Taskforce

Bereits im März 2023 hatte der EDSA die Einrichtung einer Taskforce beschlossen, die sich mit der Verarbeitung personenbezogener Daten beim Einsatz von Chat GPT befassen soll. Wesentliches Recherche-Instrument war dabei ein Fragebogen, den alle beteiligten nationalen Aufsichtsbehörden benutzt haben. Der Fragebogen bietet wertvolle Anhaltspunkte dafür, worauf Datenschutzbeauftragte zu achten haben, wenn sie den Einsatz von Chat GPT beurteilen. Er ist in dem nun vorgelegten Bericht als Anhang enthalten.

Vorläufiger Charakter des Berichts

Der Bericht des EDSA hat vorläufigen Charakter, weil die Ermittlungen der nationalen Aufsichtsbehörden noch andauern. Sein Kernstück bilden die vorläufigen Feststellungen dazu, ob beim Einsatz von Chat GPT die Einhaltung der Vorgaben der DSGVO zu gewährleisten ist (siehe dazu Teil 3 des Berichts). Insgesamt fallen die Feststellungen recht allgemein aus. Oft wirken sie eher wie Appelle, so etwa bei der Ermahnung, es sei zwingend erforderlich, dass betroffene Personen ihre Rechte auf einfache Weise ausüben können (Rn 33 des Berichts).

Quelle: European Data Protection Board (EDPB), Report of the work undertaken by the ChatGPT Taskforce, veröffentlicht am 23. Mai 2024. Der nur in englischer Sprache verfügbare Bericht hat einen Umfang von 14 Seiten. Er ist abrufbar unter https://ogy.de/xkxr.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken und seit vielen Jahren als Autor und Referent im Datenschutz erfahren.

Bild: iStock/shansekala

Nutzen Sie diesen Beitrag als gute Gelegenheit, das eigene Bewerbungsmanagement zu prüfen: Inwieweit sind dort Ziele und Zwecke angemessen definiert?

Grundsätze der Datenverarbeitung (Teil 5)

Das bedeutet der Grundsatz der Zweckbindung in der Praxis

Eine zentrale Vorschrift der Datenschutz-Grundverordnung (DSGVO) ist der Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 Buchst. b. Doch wie lässt sie sich Zweckbindung in der Praxis umsetzen?

Wer die Zweckbindung erfüllen muss, braucht eine Zweckbestimmung, die vorher erfolgt sein muss. Um Zwecke bestimmen zu können, müssen Ziele definiert sein. Dass ein Unternehmen dabei personenbezogene Daten verarbeitet, macht diese Abläufe relevant für den Datenschutz.

Praxisbeispiel Bewerbungsmanagement

Das Bewerbungsmanagement verfolgt mehrere Ziele:

- sich bewerbende Personen effizient auswählen,
- den Rekrutierungsablauf optimieren,
- das Unternehmen attraktiv für Bewerbende machen und
- dabei alle rechtlichen Vorgaben wie den Datenschutz einhalten.

Die Verarbeitungstätigkeiten im Bewerbungsmanagement können unterschiedlichen Zwecken dienen:

- die Bewerbenden auszuwählen und zu bewerten,
- mit Bewerbenden zu kommunizieren,
- den Auswahlprozess zu dokumentieren,
- alle Compliance-Vorgaben zu erfüllen,
- Verarbeitungsschritte im Rekrutierungsprozess zu optimieren und
- geeignete Bewerbende für künftige Stellenangebote zu berücksichtigen.

Weitere legale Ziele und Zwecke können hinzukommen. Das Unternehmen muss diese aber festlegen, bevor der jeweilige Verarbeitungsprozess beginnt.

Zweckbestimmung und Zweckbindung – was ist das?

Begriffe sind allerdings immer wieder unterschiedlich definiert. Daher versuchen wir hier, das zu klären.

Zweckbestimmung und Zweckbindung sind eng miteinander verknüpft, aber nicht identisch. Die Zweckbestimmung beschreibt den konkreten Grund, warum ein Unternehmen personenbezogene Daten erhebt und verarbeitet. Diese Zwecke muss das Unternehmen definieren und kommunizieren, bevor es Daten verarbeitet.

Zweckbindung hingegen bedeutet, dass das Unternehmen die erhobenen Daten nur für die ursprünglich festgelegten Zwecke nutzen darf. Unter bestimmten Bedingungen ist es aber erlaubt, die Daten für andere Zwecke weiterzuverarbeiten. Beim hier besprochenen Grundsatz geht es lediglich um die Zweckbindung. Die Zweckbestimmung wird vorausgesetzt.

Beispiel: Videoüberwachung des Firmengeländes

Ein praktisches Beispiel hilft, diese Begriffe zu verdeutlichen: Stellen Sie sich vor, ein Unternehmen installiert nach wiederholten unschönen Vorfällen Videoüberwachungskameras an den Außengrenzen des Firmengeländes. Die Zweckbestimmung könnte lauten: „Die Videoüberwachung dient dazu, das Hausrecht zu wahren, die Sicherheit der Mitarbeitenden und Besuchenden zu garantieren sowie das Eigentum vor unbefugtem Zutritt, Vandalismus und Diebstahl zu schützen." Diese Festlegung muss das Unternehmen den betroffenen Personen kommunizieren, etwa durch Hinweisschilder und Datenschutzerklärungen.

Die Zweckbindung stellt sicher, dass das Unternehmen die aufgezeichneten Daten ausschließlich verwendet, um diese Zwecke zu erfüllen. So wäre es beispielsweise unzulässig, die Aufnahmen zu nutzen, um die Pausenzeiten der Belegschaft zu überwachen. Denn dies ist nicht mit dem →

ursprünglichen Zweck vereinbar. Hierüber müssen sich alle Personen, die am Prozess beteiligt sind, im Klaren sein.

Dokumentation und Rechenschaftspflicht

Es ist aber nicht allein damit getan, Ziele, Zweckbestimmung und Zweckbindung festzulegen. Das Unternehmen muss darüber auch Nachweise vorlegen können.

Ein zentrales Element der Zweckbindung ist die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO: Verantwortliche müssen nachweisen können, dass sie personenbezogene Daten gemäß den festgelegten Zwecken verarbeiten. Dies erfolgt u.a. durch das Verzeichnis von Verarbeitungstätigkeiten. Dieses enthält detaillierte Informationen über die Verarbeitungsprozesse einschließlich der Zwecke sowie der technischen und organisatorischen Maßnahmen (TOMs).

Beispiel: Bonitätsprüfung von Kundinnen und Kunden

Ein weiteres Beispiel ist die Bonitätsprüfung. Hier definiert ein Unternehmen die Zweckbestimmung möglicherweise so: „Die Bonitätsprüfung dient dazu, das Risiko beim Kauf auf Rechnung zu minimieren." Das Unternehmen muss seine Kundschaft darüber informieren, dass es ihre Daten für diesen Zweck verwendet.

Diese Information sollte das Unternehmen in den allgemeinen Geschäftsbedingungen aufführen. Zudem muss sie in den Datenschutzerklärungen enthalten sein. Das Unternehmen darf die Daten dann gemäß der Zweckbindung auch nur für die Bonitätsprüfung verwenden.

Technische und organisatorische Maßnahmen (TOMs)

Ein Unternehmen muss sicherstellen, dass es die Anforderung der Zweckbindung erfüllt. Dazu sind geeignete TOMs nötig.

Dies umfasst z.B., Videoaufzeichnungen und Daten zur Bonitätsprüfung zu verschlüsseln. Zudem muss das Unternehmen Zugriffskontrollen einrichten. So stellt es sicher, dass nur berechtigte Personen Zugang zu den Daten haben, soweit dies erforderlich ist, um die Zwecke der Datenverarbeitung zu erfüllen.

Wenn sich Zwecke ändern oder neue hinzukommen

Sind die Prozesse bekannt sowie richtig dokumentiert, sollten auch die Zweckbestimmung und die -bindung funktionieren. Allerdings ergeben sich immer wieder Fälle, die vorhandene Daten für weitere, nicht definierte Zwecke erfordern.

Beispiel Videoüberwachung

Ein Fahrzeug fährt nachts auf das Firmengelände und die Eindringlinge begehen mutmaßlich einen Diebstahl. Der Wachdienst ruft die Polizei. Diese möchte die Videoaufnahmen der Überwachungskameras sehen, um die Fahndung nach den Kriminellen zu beschleunigen.

Die Zweckbestimmung der Videoüberwachung führt jedoch die Ermittlungen bei Verdacht auf Straftaten nicht ausdrücklich auf. Zudem besagt eine Betriebsvereinbarung, dass der Betriebsrat immer hinzuzuziehen ist, wenn der Verdacht besteht, dass Beschäftigte beteiligt sein könnten.

Will das Facility-Management hier alles richtig machen, sollte es überprüfen: Ist es gerechtfertigt, die Videoaufnahmen zu nutzen, um die Polizeiermittlungen im Rahmen der ursprünglichen Zwecke (Schutz vor Diebstahl) zu unterstützen? Damit wird es regelmäßig überfordert sein.

ACHTUNG!

Trotz aller Vorkehrungen kann es dazu kommen, dass ein Unternehmen gegen die Zweckbindung verstößt. Wichtig ist, diese Verstöße zeitnah zu erkennen, zu dokumentieren und geeignete Maßnahmen zu ergreifen, um sie zu beheben. Ein Unternehmen sollte jede Abweichung als Lernchance nutzen, um die Datenschutzprozesse kontinuierlich zu verbessern.

Außerdem: Lässt sich nicht ausschließen, dass Mitarbeitende beteiligt sein könnten, muss das Facility-Management gemäß der Betriebsvereinbarung den Betriebsrat hinzuziehen.

Bis die erforderlichen Schritte erfolgt sind und die Polizei die Ermittlungen fortführen kann, dürften die Kriminellen, falls sie besagtes Fahrzeug benutzt haben, über alle Berge sein. Denkbar wäre auch ein richterlicher Beschluss, aber dieser dauert ebenfalls seine Zeit.

In der Praxis wird ein solches Erlebnis dazu führen, das die Zweckbestimmung erweitert wird. Dies muss dann allerdings mit allen erforderlichen Schritten erfolgen. Das Unternehmen muss also seine Datenschutzinformationen ergänzen und den Betriebsrat beteiligen. Schließlich wollte dieser sicher nicht, dass die Betriebsvereinbarung Kriminelle schützt. Außerdem muss das Unternehmen alle am Prozess beteiligten Personen informieren.

Es ergibt absolut Sinn, dass sich Datenschutzbeauftragte im Rahmen ihrer Überwachungstätigkeit rechtzeitig darum kümmern, dass die Prozesse stimmig sind.

Fazit und Ausblick

Der Grundsatz der Zweckbindung ist ein zentraler Pfeiler der DSGVO. Er stellt sicher, dass eine Organisation personenbezogene Daten nur für legitime und eindeutig definierte Zwecke verarbeitet. Indem Unternehmen die Prinzipien der Zweckbindung konsequent umsetzen, schützen sie nicht nur die Daten betroffener Personen, sondern stärken auch das Vertrauen in ihre Datenschutzaktivitäten.

Die Zweckbindung umzusetzen, erfordert ein umfassendes Verständnis der Datenschutzvorschriften, angemessene Dokumentation, geeignete technische und organisatorische Maßnahmen sowie regelmäßige Schulungen.

Eberhard Häcker ist seit vielen Jahren selbstständig und davon überzeugt, dass dass seine Zweckbestimmung der Datenschutz ist..

Bild: iStock/laddawan punna

SASE bietet eine einheitliche und umfassende Sicherheitslösung, die den modernen Anforderungen an Flexibilität und Sicherheit gerecht wird. Worauf Sie als DSB achten sollten, erfahren Sie in diesem Beitrag.

Keine Cybersicherheit ohne Datenschutz (Teil 2)

Bessere User Experience, weniger Privatsphäre?

In Zeiten dezentraler Arbeit in Homeoffices und unterwegs sollen Konzepte wie Secure Access Service Edge (SASE) einen verbesserten, sicheren und nahtlosen Zugriff auf Cloud-Dienste und Netzwerkressourcen ermöglichen. Das könnte den Datenschutz aushöhlen.

Sollen an jedem Ort und zu jeder Zeit Daten zugänglich sein, die früher gut geschützt im Unternehmensnetzwerk lagen, stellt dies hohe Anforderungen an die Datensicherheit. Konzepte wie Zero Trust sollen mit risikoabhängigen Zugriffskontrollen für den notwendigen Schutz sorgen (zu Zero Trust siehe Ausgabe 07/2024, S. 18).

Doch nicht nur die Sicherheit ist durch die dezentrale Arbeit stärker gefordert als zuvor, auch die Netzwerke müssen höheren Maßstäben gerecht werden. Die Daten sollen überall schnell verfügbar und die Anwendungen performant sein. Sonst sinkt die Produktivität und das Nutzererlebnis, neudeutsch User Experience, leidet.

Marktforscher wie Gartner (https://ogy.de/squw) sehen in SASE eine zentrale Lösung für dieses Problem. Hinter dem Konzept steckt die Idee, alle Sicherheits- und Netzwerkfunktionen für dezentrales Arbeiten zu vereinen. Gartner definiert SASE als „konvergierte Netzwerk- und Security-as-a-Service-Funktionen" (https://ogy.de/vnu6).

Das Ziel: Überall produktiv und sicher arbeiten

SASE unterstützt demnach Anwendungsfälle für den sicheren Zugriff in Zweigstellen, bei Remote-Mitarbeitern und vor Ort.

SASE läuft in erster Linie als Service und ermöglicht einen geschützten Zugriff. Dieser basiert auf der Identität des Geräts oder der Person, kombiniert mit aktuellen Informationen zur Nutzung sowie Sicherheits- und Compliance-Richtlinien.

Doch was bedeutet das für die Privatsphäre? Für den Datenschutz ist es natürlich positiv, wenn die Fernzugriffe auf Daten und Anwendungen sicherer und zuverlässiger erfolgen. Es ist aber zu bedenken, wie SASE für das genannte gute und sichere Nutzererlebnis sorgen soll, denn dies kann sich negativ auf den Datenschutz auswirken.

SASE soll liefern, was man braucht

Da die verfügbaren Netzwerkverbindungen und -geschwindigkeiten nicht unbegrenzt sind, sondern oftmals eher stark limitiert, gilt es Prioritäten zu setzen: Jede Nutzerin und jeder Nutzer soll auf die Anwendungen und Daten, die gerade notwendig sind, zugreifen können.

Die Komponenten von Secure Access Service Edge (SASE)

Das gehört zu SASE

SASE ist eine Kombination aus Lösungen, die verknüpft und übergreifend zu administrieren sind:

- Software-defined WAN (SD-WAN) für die Netzwerkfunktionen
- sicheres Web-Gateway für den geschützten Web-Zugang
- sicherer Netzzugang (Zero Trust)
- Funktionen für die Cloud-Sicherheit
- Firewall-as-a-Service (Firewall-Dienstleistungen)

Weil Einrichtung und Betrieb komplex sind, kümmert sich häufig ein Service-Provider darum (Managed SASE).

→

Dazu muss eine SASE-Lösung wissen, wer was wann in welchem Umfang benötigt. Nur dann kann sie die Sicherheits- und Netzwerkfunktionen passend bereitstellen. Dieses Wissen zur richtigen Priorisierung darf aber nicht zu weit gehen.

SASE und User Analytics

Um die jeweils erforderlichen Verbindungen, Anwendungen und Daten zur Verfügung stellen zu können, werten SASE-Lösungen die Datenmengen aus. Sie ermitteln die Bandbreiten, die die Applikationen und Dienste benötigen. Daraus leiten sie Trends ab, um schnell auf den Bedarf reagieren zu können.

Doch die Lösungen analysieren nicht nur Datenpakete, sondern unterziehen auch die Nutzerinnen und Nutzer einer genauen Untersuchung. Dabei ermitteln sie, wer wann welche Anwendung und welchen Dienst benötigt. Auf dieser Grundlage kann SASE die zugehörigen Verbindungen und Funktionen priorisieren und bereitstellen. Heraus kommt ein Normalverhalten, um dann Anomalien als mögliche kriminelle Aktivität feststellen zu können:

- Erfolgen Zugriffe zu ungewöhnlichen Uhrzeiten?
- Weicht der Datenverkehr deutlich von üblichen Werten ab?

Die Nutzungsstatistiken helfen dabei, Kapazitäten im weit verzweigten Netzwerk zu planen und mögliche Angriffe zu erkennen, doch sie könnten dabei den Datenschutz aushöhlen.

KI in SASE-Lösungen

Zur Analyse des Datenverkehrs und der Nutzeraktivitäten kommt zunehmend künstliche Intelligenz (KI) zum Einsatz. Das verwundert nicht, da KI-Services besonders im Bereich der Mustererkennung erfolgreich und erprobt sind. Sie eignen sich somit, ein Normalverhalten zu bestimmen und Anomalien zu identifizieren.

Zudem lassen sich Funktionen und Verbindungen als Reaktion auf einen neuen Bedarf sehr schnell umsetzen – gut für die Produktivität, aber womöglich nachteilig für den Datenschutz.

Nicht anonymisierte personenbezogene Daten könnten Teil der Trainingsdaten werden, mit oftmals unklaren Folgen mangels Transparenz vieler KI-Dienste.

SASE aus der Cloud oder im Eigenbetrieb

Bei unzureichendem Datenschutz können personenbezogene Daten nicht nur einer KI zufallen. Da es sehr komplex sein kann, SASE einzurichten und zu betreiben, entscheiden sich viele Unternehmen für eine SASE-Lösung aus der Cloud.

Dann aber könnten die Nutzerdaten in einer Cloud landen, womöglich jenseits von EU bzw. EWR, sodass Rechtsgrundlagen und das Datenschutzniveau am Ort der Cloud und beim Provider zu klären sind.

Man kann sich bei SASE auch für den Eigenbetrieb entscheiden. Die Integration der Einzellösungen und die Konfiguration innerhalb des SASE-Konzepts sind nicht trivial, sodass das Risiko besteht, Konfigurationsfehler zu begehen. Dadurch könnten Schwachstellen im Netzwerk entstehen, die leicht zu übersehen sind, die Angreifer aber ausnutzen könnten.

Prüffragen	Ja	Nein
Haben Sie geprüft, ob die Daten der Nutzenden anonymisiert wurden, bevor die Auswahl und Priorisierung der Sicherheits- und Netzwerkfunktionen erfolgt?	☐	☐
Ist sichergestellt, dass der Verantwortliche die Auswertungen nicht zu anderen Zwecken einsetzt wie Leistungs- und Verhaltenskontrollen?	☐	☐
Ist gewährleistet, dass mögliche KI-Funktionen innerhalb der SASE-Lösung keinen Zugriff auf personenbezogene und andere vertrauliche Daten erhalten?	☐	☐
Finden mögliche Datenübermittlungen an den Cloud-Provider (SASE aus der Cloud, Managed SASE) auf einer Rechtsgrundlage statt?	☐	☐
Ist sichergestellt, dass die IT bei Einrichtung und Verwaltung der einzelnen Sicherheits- und Netzwerkfunktionen die Konfigurationen überprüft, um Sicherheitslücken zu vermeiden?	☐	☐

Datenschutz-Prüfungen bei der Planung von SASE

Oliver Schonschek, Dipl.-Phys., ist News Analyst mit Fokus auf IT-Sicherheit und Datenschutz und Co-Host von Datenschutz PRAXIS Der Podcast. Auch 2024 wurde er als Top 10 Global Thought Leader für Privacy, Security und Cybersecurity ausgezeichnet.

PRAXIS-TIPP

Bevor Konzepte wie SASE zum Einsatz kommen, sind die Auswirkungen auf den Datenschutz zu prüfen. Da SASE mehrere Sicherheits- und Netzwerkfunktionen kombiniert, sind zahlreiche Kontrollen erforderlich in den Bereichen Firewall, Netzwerksicherheit, Cloud-Sicherheit und Web-Sicherheit. In allen Bereichen sollten Datenschutzbeauftragte dabei insbesondere diese Punkte hinterfragen:

- *User Analytics: Anonymisierung, Zweckbindung, Datenminimierung*
- *Nutzung von künstlicher Intelligenz (KI): Transparenz, mögliche KI-Risiken*
- *Cloud-Provider: Datenschutzniveau, Rechtsgrundlage bei Datenübermittlung*
- *Alternativer Eigenbetrieb: Gewährleistung von Einrichtung, Betrieb und Wartung, Datenschutz und Datensicherheit*

Nur wenn der Datenschutz bei SASE selbst stimmt, kann SASE zu einer sicheren und datenschutzkonformen dezentralen Arbeit beitragen. Andernfalls könnte SASE ungewollte und unerlaubte Einblicke in die Aktivitäten der Nutzenden bieten – überall und zu jeder Zeit.

Bild: iStock/metamorworks

Was die Umsetzung des DSA in deutsches Recht für Ihre Praxis als DSB bedeutet und wo Sie handeln sollten, erläutert Dr. Eckhardt in diesem Beitrag

Was die Änderungen für den Datenschutz bedeuten

Aus TTDSG wird TDDDG und aus TMG wird DDG: Und jetzt?

Gerade hatten Sie sich an das Telekommunikation-Telemedien-Datenschutzgesetz gewöhnt, schon heißt es Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz. Und das Digitale-Dienste-Gesetz ersetzt das Telemediengesetz. Aber was ändert sich außer den Namen?

Alles neu macht der Digital Services Act (DSA) – unmittelbar, mittelbar und doch nicht ganz. So lässt sich die Auswirkung des DSA im deutschen Recht umschreiben.

Alles neu macht der Digital Services Act (DSA)

Klingt komplex, lässt sich aber nachvollziehen: Der DSA regelt als EU-Verordnung direkt und unmittelbar in allen EU-Mitgliedstaaten die sogenannten Dienste der Informationsgesellschaft und insbesondere die (Begrenzung der) Haftung für Inhalte im Onlinebereich neu. Das war bisher im Telemediengesetz (TMG) geregelt. Aufgrund des Vorrangs des DSA wurden diese Regelungen im TMG obsolet und mussten aufgehoben werden. Hier entsteht für den Datenschutzbeauftragten kein originärer Handlungsbedarf.

Aber nicht alle Inhalte des bisherigen TMG wurden überflüssig. Die Regelung z.B. zum Impressum wird durch den DSA nicht geändert. Diese beruhen auf einer älteren EU-Richtline. Die Inhalte des bisherigen TMG ließen sich daher nicht „in Bausch und Bogen" einfach aufheben.

Gleichzeitig macht der DSA auch neue Regelungen im deutschen Recht etwa in bezug auf Zuständigkeiten erforderlich. Der Gesetzgeber musste also zusätzlich aktiv werden.

Das Netzwerkdurchsetzungsgesetz (NetzDG) wurde ebenfalls überflüssig, weil der Digital Services Act auch das Vorgehen gegen rechtswidrige Inhalte im Internet regelt.

Der deutsche Gesetzgeber hat hierzu das neue Digitale-Dienste-Gesetz (DDG) geschaffen. Die neuen Regelungen knüpfen – entsprechend dem DSA – nicht mehr an Telemedien, sondern an Digitale Dienste an. Auch wenn das nur nach einer Begrifflichkeit aussieht, hat v.a. diese neue Begrifflichkeit Auswirkungen.

Auswirkungen des DSA auf die Datenschutzgesetze

Obwohl der DSA kein Datenschutzrechtsakt ist, hatte die vorstehende Änderung auch Auswirkungen auf die Datenschutzregelungen des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG).

Zum Verständnis: Die Datenschutzbestimmungen aus dem TMG wurden zum 01.12.2021 im TTDSG mit den Telekommunikationsdatenschutzbestimmungen zusammengeführt. Das TTDSG regelte also als „Annex" den Datenschutz für Telemedien (und für Telekommunikation).

Mit der Änderung von Telemedien zu Digitale Dienste musste der Gesetzgeber daher auch das TTDSG in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ändern.

(Neu-)Regelung der Impressumspflicht im DDG

Das für die Praxis bedeutsame – und häufig in die Beratung durch DSB wegen der Überschneidung zur Benennung des Verantwortlichen einbezogene – Impressum ist nicht durch den DSA inhaltlich neu geregelt worden. Die alte Regelung von § 5 TMG-alt wird in § 5 DDG fortgeführt. Hier entsteht Handlungsbedarf (siehe Praxis-Tipp)!

PRAXIS-TIPP

Was bedeutet das für die Praxis?
Sie müssen für das Impressum die Bezugnahme auf „§ 5 TMG" durch eine Bezugnahme auf „§ 5 DDG" ersetzen. Sie sollten aber diese Gelegenheit auf jeden Fall zur Prüfung nutzen, ob tatsächlich die Pflichtangaben von § 5 DDG genannt werden.
Jeder Anbieter digitaler Dienste (§ 1 Abs. 4 Nr. 5, Nr. 1 DDG) muss zwar nach § 5 DDG die dort genannten Pflichtangaben machen. Anders als nach Art. 13, 14 DSGVO muss er aber keine Rechtsgrundlage nennen. Er kann die Pflicht also auch erfüllen, wenn er „§ 5 DDG" nicht ausdrücklich anführt.

Digitale Dienste statt Telemedien

Mit der Abschaffung des TMG führt der Gesetzgeber eine neue Begrifflichkeit ein und damit zugleich (endlich) eine Vereinheitlichung zum EU-Recht herbei.

Das EU-Recht kennt keine Telemedien. Diese waren seit den 1990iger-Jahren eine „Sonderlocke" des deutschen Rechts. Das führte zu Friktionen mit dem EU-Recht, die nunmehr entfallen. Aber: Das ist nicht nur eine Änderung des Begriffs. Beide Begriffe sind auch unterschiedlich definiert.

Für die Praxis bedeutet das: Der Anwendungsbereich der Regelungen – also auch etwa die Impressumspflicht – ändert sich. Das muss nicht zwingend zu Änderungen führen, kann es aber. Prüfen Sie das!

Digitale Dienste und Dienst der Informationsgesellschaft

Der deutsche Gesetzgeber verwendet im DDG (und damit im TDDDG) aber nicht einfach den Begriff „Dienst der Informationsgesellschaft", wie ihn der maßgebliche DSA in Art. 3 Nr. 1 DSA definiert, sondern den Begriff „Digitale Dienste".

Wenn das DDG denselben Begriff wie der DSA verwendet hätte, wäre es zwar einfacher gewesen, aber jedenfalls gibt es keine inhaltlichen Unterschiede. Damit wird es leider auch direkt wieder komplizierter, weil es nun auf die Verweisungen in den Gesetzen ankommt:

Der DSA nimmt für seinen Begriff „Dienst der Informationsgesellschaft" in Art. 3 Nr. 1 DSA Bezug auf die Definition in Art. 1 Abs. 1 Buchst. b der Richtlinie (EU) 2015/1535. Das DDG nimmt für seinen „digitaler Dienst" in § 1 Abs. 4 Nr. 1 DDG ebenfalls Bezug auf diese Definition in Art. 1 Abs. 1 Buchst. b der Richtlinie (EU) 2015/1535.

Damit ist die Definition in Art. 1 Abs. 1 Buchst. b der Richtlinie (EU) 2015/1535 von zentraler Bedeutung für den DSA, das DDG und das TDDDG.

Aus TTDSG wird TDDDG

Das TTDSG wurde durch die Änderung in das TDDDG nicht grundlegend geändert. Der weiterhin im zweiten Teil des TDDDG geregelte Telekommunikationsdatenschutz bleibt – was schon die begriffliche Änderung nahelegt – durch diese Änderung unberührt. Auch die inhaltliche Trennung zwischen Teil 2 (Telekommunikation) und Teil 3 (Digitale Dienste bzw. vormals Telemedien) ist nicht aufgehoben.

Für den Teil 3 (Digitale Dienste bzw. vormals Telemedien) ergeben sich Änderungen. Diese zeigen sich aber nicht in geänderten Regelungen, da der DSA hierfür auch keine Änderungen erzwingt.

Die Änderungen im Teil 3 ergeben sich mittelbar dadurch, dass er nun für Digitale Dienste (siehe oben) gilt, also für etwas anderes als die bisher geregelten Telemedien.

Das TDDDG nimmt die Anbieter digitaler Dienste in die Pflicht. „Anbieter von digitalen Diensten" ist nach § 2 Abs. 2 Nr. 1 TDDDG „jede natürliche oder juristische Person, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt". Zwar hat der Gesetzgeber in dieser Definition lediglich den Begriff „Telemedien" durch „digitale Dienste" ersetzt. Für den Begriff „digitale Dienste" gilt gemäß § 2 Abs. 1 TDDDG aber die bereits oben dargestellte neue Begriffsbestimmung des DDG.

Der Begriff „Digitale Dienste" ist sowohl für das DDG als auch das TDDDG von zentraler Bedeutung!

Die Definition von „Digitale Dienste" in Art. 1 Abs. 1 Buchst. b der Richtlinie (EU) 2015/1535 lautet:
„eine Dienstleistung der Informationsgesellschaft, d.h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.
Im Sinne dieser Definition bezeichnet der Ausdruck
i) „im Fernabsatz erbrachte Dienstleistung" eine Dienstleistung, die ohne gleichzeitige physische Anwesenheit der Vertragsparteien erbracht wird;
ii) „elektronisch erbrachte Dienstleistung" eine Dienstleistung, die mittels Geräten für die elektronische Verarbeitung (einschließlich digitaler Kompression) und Speicherung von Daten am Ausgangspunkt gesendet und am Endpunkt empfangen wird und die vollständig über Draht, über Funk, auf optischem oder anderem elektromagnetischem Wege gesendet, weitergeleitet und empfangen wird;
iii) „auf individuellen Abruf eines Empfängers erbrachte Dienstleistung" eine Dienstleistung die durch die Übertragung von Daten auf individuelle Anforderung erbracht wird."
Die Richtlinie (EU) 2015/1535 enthält in ihrem Anhang I eine Beispielliste der nicht (!) unter diese Definition fallenden Dienste. Diese kann als Orientierung in der Praxis dienen.

Konsequenzen der Änderung von TTDSG-alt zu TDDDG für die Praxis

Auch wenn mit dem Wechsel keine – jedenfalls keine wesentlichen – Änderungen erfolgen, zeigt sich in der Regelung zum Schutz der Privatsphäre in § 25 TDDDG (Stichwort: Cookie-Regelung) doch eine Anpassung. Denn die Ausnahme in § 25 Abs. 2 Nr. 2 TDDDG nimmt ebenfalls nicht mehr Bezug auf Telemedien, sondern auf Digitale Dienste. Hier kann sich die neue Begrifflichkeit auswirken!

Soweit in der Praxis § 25 Abs. 2 Nr. 2 TTDSG-alt allerdings bereits bisher richtlinienkonform entsprechend der Richtlinie 2009/136/EG zur Änderung von Art. 5 Abs. 3 Richtlinie 2002/58/EG ohnehin als „Dienst der Informationsgesellschaft" ausgelegt wurde, ändert sich nichts. Hier zeigt sich, dass der Gesetzgeber nunmehr Friktionen zum EU-Recht aufgelöst hat.

Die Informationspflichten der Art. 13, 14 DSGVO gelten auch für Anbieter digitaler Dienste bei der Verarbeitung personenbezogener Daten. Hat ein Diensteanbieter nach Art. 13 Abs. 1 Buchst. c, 14 Abs. 1 Buchst. c DSGVO bisher eine Regelung des TTDSG (insbesondere § 25 TTDSG) genannt, dann muss er dies nunmehr ändern: Er muss das TDDDG nennen. Im Übrigen werden die Auswirkungen für den Datenschutz überschaubar sein. Denn schon bisher galten für die Telemedien und jetzt für die Digitalen Dienste im Wesentlichen die Datenschutzbestimmungen der DSGVO.

Für die Zugriffsbefugnisse der Sicherheitsbehörden nach § 22 bis 24 TDDDG wird sich der geänderte Anwendungsbereich stärker auswirken und zukünftig eine konkrete Prüfung erfordern. Das müssen v.a. die fachkundigen Personen nach § 22, 24 TDDDG, die die Auskunftsverlangen prüfen müssen, beachten.

WICHTIG

Prüfen Sie die Datenschutzhinweise und v.a. die Datenschutzrichtlinien auf den Internetseiten, ob die aktuellen Regelungen genannt sind.
Nutzen Sie die Gelegenheit, um kritisch zu prüfen, ob die richtige Rechtsgrundlage genannt ist. Denn § 25 TDDDG ist (und war) keine Rechtsgrundlage, um personenbezogene Daten zu analysieren, sondern nur für den Zugriff oder die Speicherung von Informationen in der Endeinrichtung des Endnutzers. Prüfen Sie die aktuellen Rechtsentwicklungen! Auch auf die Cookie-Regelung wirkt sich das aus. Denn bisher galt die Ausnahme von § 25 Abs. 2 Nr. 2 TTDSG-alt für Telemediendienste. Nunmehr gilt sie für digitale Dienste.

Fazit

Es besteht Handlungsbedarf. Diese Gelegenheit sollten Sie nutzen, um das Impressum sowie die datenschutzrechtlichen Pflichthinweise zu prüfen und ggf. zu aktualisieren. Denn die Praxis zeigt leider, dass solche Änderungen auch Anlässe für Abmahnwillige sind!

Dr. Jens Eckhardt ist Rechtsanwalt und Partner bei pitc legal Eckhardt Rechtsanwälte Partnerschaft mbB in Düsseldorf.

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
Andreas Dumont, München
Dr. Wilhelm Greiner, Mitteilerei

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 0 82 33.23-5 72 68
E-Mail: anton.sigllechner@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 279 € (zzgl. MwSt. und Versandkosten)
12 Ausgaben als PDF im Heftarchiv + Online-Zugriff 269 € (zzgl. MwSt.)

Druck:
Burscheid Medien GmbH
Leonhardstraße 23, 88471 Laupheim

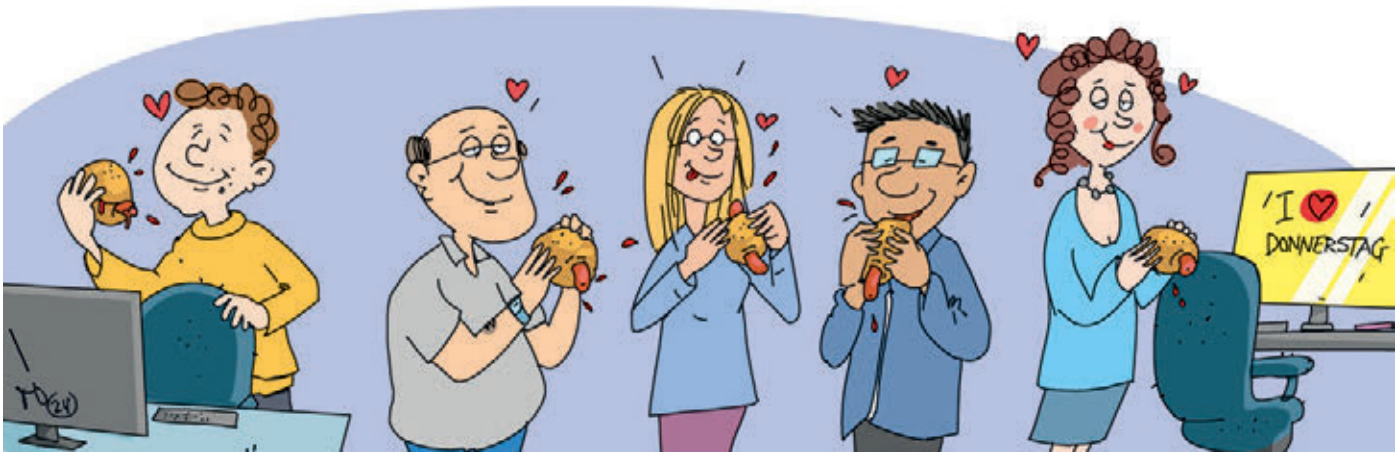
Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4127

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.



Vom Homeoffice zurück ins Büro

Spitzen-Hotdogs am Donnerstag – und das Büro ist wieder voll

Immer mehr Unternehmen suchen nach einfachen Wegen, die Beschäftigen wieder öfter ins Büro zu holen. Aber Homeoffice ist in vielen Fällen angenehmer. Also gilt es, die Belegschaft mit kreativen Ideen fürs Büro zu motivieren – manchmal mit positiven Folgen für Datenschutzbeauftragte, die vor Ort prüfen.

Die Geschäftsleitung hatte lange überlegt, wie sie mehr Beschäftigte aus dem Homeoffice ins Unternehmen locken könnte. Obwohl Projektmitarbeitende nur zwei Tage im Monat im Büro sein mussten, sollten sie mindestens viermal, besser öfter, erscheinen. Die Chefetage rief die Teamleitungen zusammen. Kollege Breitkreuz, ein Liebhaber guten Essens (man sieht es), hatte die Idee.

Eine zündende Idee

„An welchem Wochentag sollen denn möglichst viele Personen da sein?", fragte er. Die Antwort: am Donnerstag. Breitkreuz erinnerte an einen Imbiss in der Nachbarschaft, der göttliche Hotdogs in gefühlt 20 Variationen anbot. Früher gingen die Kolleginnen und Kollegen immer dorthin zum Mittagessen.

Sein nicht ganz uneigennütziger Vorschlag: „Lasst uns jeden Donnerstag Hotdogs von diesem Imbiss im Büro kostenlos verteilen. Der Rest kommt von allein." Die Geschäftsführung setzte die Idee um.

Zur Nachahmung empfohlen!

Die Hotdog-Donnerstage wurden schnell zum Highlight der Woche. Mitarbeitende kamen nicht nur wegen der köstlichen Hotdogs ins Büro, sondern auch, um sich wieder persönlich auszutauschen und die Gemeinschaft zu erleben. Mal abgesehen davon, ob das jetzt gesund ist oder nicht: Hauptsache lecker. Zumal es auch einen veganen Hotdog gibt. Prädikat: zur Nachahmung empfohlen!

Nachtrag: Natürlich war ich an einem Donnerstag bei meiner Datenschutz-Begehung vor Ort. Fast alle Arbeitsplätze besetzt. Meine Begehungen werden dort künftig donnerstags stattfinden. Danke, Kollege Breitkreuz. Die Hotdogs sind genial. Und bis ich alle 20 Variationen durchhabe, wird es noch eine Weile dauern …

Eberhard Häcker ist seit vielen Jahren selbstständig und mit großer Leidenschaft sowie Kreativität externer Datenschutzbeauftragter

In der nächsten Ausgabe

KI & Datenschutz

Das empfiehlt die Orientierungshilfe der Datenschutzkonferenz für den datenschutzkonformen Einsatz von KI.

Neues aus Tätigkeitsberichten

Die Fälle, die die Aufsichtsbehörden in ihren Berichten dokumentieren, bieten wertvolle Erkenntnisse für die Praxis.

DSB & KI-Beauftragter?

Wir beleuchten Interessenkonflikte von DSB, insbesondere im Hinblick auf die Benennung als KI-Beauftragter.