

Datenschutz Radar

Eine Ausgabe von DSBOK.de | September 2026

INHALT :

■ Seite 2

Digitale Souveränität – warum sie für den Datenschutz wichtig ist

■ Seite 5

Sicherheitsüberprüfung von Beschäftigten – wer wird geprüft und warum?

■ Seite 7

Personalausweis kopieren – oft gemacht, aber erlaubt?

■ Seite 9

Gestohlene Daten: Der Angriff endet nicht mit dem Hack

Wir brauchen Unabhängigkeit

Viele grundlegende Technologien und Dienste stammen nicht aus Deutschland oder der EU. Technologische Abhängigkeiten sind ein strategisches Risiko. In vielen Bereichen dominieren wenige große Anbieter – häufig außerhalb der EU...

(Seite 2)

Liebe Leserin, lieber Leser,

Datenschutz und Datensicherheit stehen heute im Zentrum der digitalen Welt. Die zunehmende Digitalisierung nahezu aller Bereiche macht den Schutz personenbezogener Daten zu einer zentralen Aufgabe. Diese Ausgabe zeigt, warum das konkret so wichtig ist.

Sie beleuchtet die intensiv diskutierte digitale **Souveränität** und macht deutlich: Datenschutz schützt nicht nur Informationen, sondern ist auch die Grundlage für selbstbestimmtes Handeln. Ein weiterer Beitrag erklärt, welche Anforderungen bei **Sicherheitsüberprüfungen von Beschäftigten** in sensiblen Bereichen gelten. Auch der **Umgang mit Personalausweisen** im Alltag wird aufgegriffen: Wann ist das Kopieren zulässig – und wann

nicht? Der Beitrag gibt dazu klare Antworten. Zum Abschluss zeigt ein aktueller IT-Sicherheitsvorfall bei einer Hotelbuchungsplattform: Auf Datenpannen folgen oft weitere Cyberangriffe. Umso wichtiger ist es, **im Ernstfall richtig zu reagieren**.

Ich wünsche Ihnen eine interessante Lektüre! ■

Oliver Krause

Externer Datenschutzbeauftragter
Datenschutzauditor
ok@dsbok.de



Digitale Souveränität – was bedeutet das?

Die Fähigkeit, Technologien und Daten tatsächlich selbst zu kontrollieren – und nicht von einzelnen Anbietern abhängig zu sein.

■ Digitale Souveränität – warum sie für den Datenschutz wichtig ist

Wenn es um Digitalisierung geht, ist aktuell häufig von „Souveränität“ die Rede. Doch warum spielt das plötzlich eine so große Rolle – und welche Konsequenzen hat das für den Datenschutz? Eine ganze Menge.

In der Digitalisierung gibt es ein Ungleichgewicht

Ob Computer-Hardware, Mikrochips, Suchmaschinen oder Cloud-Services: Viele grundlegende Technologien und Dienste stammen nicht aus Deutschland oder der EU. Seit Jahren zeigt sich dasselbe Bild: Europa importiert mehr digitale Technologien, als es selbst exportiert.

Dieses Ungleichgewicht ist nicht nur ein wirtschaftliches Problem – es schafft konkrete Abhängigkeiten. Die jüngsten geopolitischen Krisen machen deutlich: Technologische Abhängigkeiten sind auch ein strategisches Risiko. Deshalb richtet Deutschland seine Digitalpolitik neu aus. Ziel ist mehr Eigenständigkeit und

Sicherheit – unter anderem durch europäische Kooperationen und Investitionen in Schlüsseltechnologien.

Digitale Souveränität – was bedeutet das?

Dieses Ziel lässt sich auch als digitale Souveränität beschreiben. Gemeint ist die Fähigkeit, Technologien und Daten tatsächlich selbst zu kontrollieren – und nicht von einzelnen Anbietern abhängig zu sein. Digitale Souveränität soll Vertrauen stärken, Handlungsfähigkeit sichern und Selbstbestimmung in einer vernetzten Welt ermöglichen.

IT-Sicherheitsbehörden warnen vor der Dominanz großer Anbieter

Ein wichtiger Aspekt ist die Wahlfreiheit bei digitalen Angeboten. Genau hier zeigt sich jedoch ein Problem: In vielen Bereichen dominieren wenige große Anbieter – häufig außerhalb der EU.



Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht in diesem Zusammenhang von einer möglichen „Cyber-Dominanz“: Digitale Alltagsprodukte wie PCs oder Smartphones erfassen oft mehr Daten, als vielen bewusst ist – etwa Nutzungsverhalten oder Standortinformationen.



Hinzu kommt: Diese Geräte erhalten regelmäßig Updates vom Hersteller. Das ist für die Sicherheit unverzichtbar, bedeutet aber auch, dass Hersteller erheblichen Einfluss auf die Systeme behalten. Im Extremfall könnten sie Funktionen einschränken oder Geräte unbrauchbar machen. Die Abhängigkeit von einzelnen Anbietern wird hier besonders deutlich.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland.

Wer seine Daten kontrollieren will, braucht Unabhängigkeit

Wer kontrollieren möchte, was mit den eigenen Daten geschieht, ist auf entsprechende Funktionen angewiesen – zum Beispiel auf wirksame Verschlüsselung. Wichtig ist dabei: Diese Funktionen müssen so gestaltet sein, dass sie nicht vollständig vom Anbieter kontrolliert werden.

Fehlen solche Möglichkeiten, bleibt oft nur ein Ausweg: ein anderes Produkt oder ein anderer Anbieter. Das setzt jedoch voraus, dass es überhaupt Alternativen gibt. Ohne Alternativen gibt es keine echte Wahl – und ohne Wahl keine Kontrolle über die eigenen Daten. Dann bestimmen letztlich die Anbieter, welches Datenschutzniveau möglich ist – und welches nicht.

Datenschutz gehört zur persönlichen Freiheit

Datenschutz ist mehr als eine gesetzliche Pflicht – er entscheidet darüber, wie selbstbestimmt Menschen im digitalen Raum handeln können. Er trägt dazu bei, die Selbstbestimmung und Freiheit im digitalen Raum zu sichern.

Wenn Datenschutz konsequent umgesetzt wird, stärken Unternehmen ihre Unabhängigkeit, verbessern Nutzerinnen und Nutzer ihre Kontrolle und gemeinsam entsteht eine Grundlage für mehr digitale Souveränität.

Die Forderung nach digitaler Souveränität, die derzeit häufig zu hören ist, ist daher immer auch eine Forderung nach mehr Kontrolle, mehr Transparenz und einem bewussten Umgang mit Daten. Deshalb gehört Datenschutz stärker in den Fokus – auch im eigenen Arbeitsalltag.

Was heißt das konkret für den Arbeitsalltag?



- *Bewusster Einsatz von Tools:*

Es sollten ausschließlich die vorgesehenen und freigegebenen Anwendungen genutzt werden. Zudem ist darauf zu achten, dass nur die Daten verarbeitet werden, die tatsächlich erforderlich sind.

- *Überprüfung von Einstellungen:*

Datenschutz- und Sicherheitseinstellungen, etwa zu Zugriffsrechten oder Datenfreigaben, sollten regelmäßig geprüft und angepasst werden.

- *Sensibilisierung für Datenverarbeitung:*

Wenn unklar ist, wie Daten verarbeitet werden oder ob ein Einsatz datenschutzkonform ist, sollte dies vorab geklärt werden. ■

Datenhoheit gehört zum Datenschutz

Ein zentraler Bestandteil digitaler Souveränität ist die Datensouveränität. Sie beschreibt die Fähigkeit, selbstbestimmt über eigene Daten zu verfügen. Dazu gehört die Kontrolle darüber, wer Daten verarbeitet, zu welchem Zweck und unter welchen Bedingungen.

Genau hier setzt der Datenschutz an: Er soll diese Kontrolle sicherstellen. Auch hier geht es darum, Transparenz zu schaffen und die Kontrolle über Daten zu sichern.

Datenschutzaufsichtsbehörden betonen deshalb die enge Verbindung beider Themen: Digitale Souveränität gewinnt zunehmend an Bedeutung, wenn es darum geht, personenbezogene Daten wirksam zu schützen.

Sicherheitsüberprüfung
Abgeschlossen

Die Teilnahme ist freiwillig

Aber ohne eine abgeschlossene Sicherheitsüberprüfung ist ein Einsatz in sicherheitsrelevanten Projekten nicht möglich. In der Praxis bedeutet das: Beschäftigte ohne Überprüfung werden in der Regel in anderen Projekten eingesetzt.

■ Sicherheitsüberprüfung von Beschäftigten – wer wird geprüft und warum?

Eine Reihe von Unternehmen ist derzeit erstmals in die Abwicklung von Aufträgen aus dem Verteidigungsbereich eingebunden. Dabei kann es vorkommen, dass die öffentliche Hand als Auftraggeber eine Sicherheitsüberprüfung von Beschäftigten verlangt. Für viele ist dieser Begriff neu. Im Folgenden wird erläutert, was dahintersteckt.

Für manche Branchen ist es Routine

In Bereichen wie der Zusammenarbeit mit der Bundeswehr oder der Polizei sind Sicherheitsüberprüfungen seit Langem üblich. Auch Beschäftigte von IT-Dienstleistern, die in diesen Bereichen tätig sind, kennen entsprechende Anforderungen.

Der Grund liegt auf der Hand: Bei solchen Aufträgen kann es erforderlich sein, auf vertrauliche oder sogar hochvertrauliche Unterlagen zuzugreifen. Öffentliche Auftraggeber müssen daher sicherstellen, dass von den beteiligten Personen keine Risiken ausgehen.

Gespielt wird mit offenen Karten

Niemand muss Sorge haben, dass solche Überprüfungen hinter seinem Rücken ablaufen – im Gegenteil. Alle Beschäftigten werden individuell darüber informiert, wenn eine Überprüfung vorgesehen ist.

Die Information erfolgt in der Regel über ein offizielles Schreiben der zuständigen Behörde, das über den Arbeitgeber weitergeleitet wird. Grundlage der Überprüfung sind standardisierte Fragen zur jeweiligen Person. Die Fragen dienen ausschließlich der Überprüfung und stellen keinen Verdacht dar. Es ist zudem möglich, die eigenen Angaben zu dokumentieren, etwa durch eine Kopie der Antworten.

Mitwirkung ist freiwillig, aber...

Die Teilnahme an einer Sicherheitsüberprüfung ist grundsätzlich freiwillig. Eine Verpflichtung zur Mitwirkung besteht nicht. Allerdings gilt: Ohne eine abgeschlossene Sicherheitsüberprüfung ist ein Einsatz in sicherheitsrelevanten Projekten nicht möglich. In der Praxis bedeutet das: Beschäftigte ohne Überprüfung werden in der Regel in anderen Projekten eingesetzt. Je nach Tätigkeit kann dies auch Auswirkungen haben, etwa wenn bestimmte Aufgaben oder Zuschläge an sicherheitsrelevante Bereiche gebunden sind.

Klare gesetzliche Grundlagen

Sicherheitsüberprüfungen sind gesetzlich geregelt. Für Bundesbehörden gilt das Sicherheitsüberprüfungsgesetz des Bundes, für Landesbehörden die entsprechenden Landesgesetze. Diese werden durch sogenannte „Verschlussachsenanweisungen“ ergänzt. Dabei handelt es sich um Verwaltungsvorschriften, die konkrete Vorgaben zur Durchführung der Überprüfungen enthalten. Die entsprechenden Regelwerke sind öffentlich zugänglich.

Arten der Sicherheitsüberprüfung und Geheimhaltungsstufen

Im Regelfall wird eine einfache Sicherheitsüberprüfung durchgeführt. Eine erweiterte Sicherheitsüberprüfung kommt zum Einsatz, wenn Tätigkeiten mit besonders sensiblen Informationen verbunden sind. Dabei spielen auch die Geheimhaltungsstufen eine Rolle. „VS – Nur für den Dienstgebrauch“ ist die niedrigste Geheimhaltungsstufe. Unterlagen mit dieser Einstufung gehören bei Bundeswehr und Polizei häufig zum Arbeitsalltag. Seltener sind Unterlagen der zweiten Geheimhaltungsstufe „VS – Vertraulich“, sie kommen aber ebenfalls vor. Die Abkürzung „VS“ steht für „Verschlussache“ und verweist darauf, dass diese Informationen besonders geschützt werden müssen.

Mit den beiden höchsten Geheimhaltungsstufen „Geheim“ und „Streng geheim“ dürften nur sehr wenige Beschäftigte im Unternehmen in Berührung kommen. Sie betreffen besonders sensible Inhalte, die selbst innerhalb von Bundeswehr, Polizei und ähnlichen Behörden nur einem sehr kleinen Personenkreis zugänglich sind.

An den Datenschutz ist gedacht

Gerade bei erweiterten Sicherheitsüberprüfungen werden auch Angaben zum persönlichen Umfeld erhoben. Dies kann einen Eingriff in das Persönlichkeitsrecht darstellen. Deshalb ist der Datenschutz ausdrücklich berücksichtigt: Die zuständigen Datenschutzaufsichtsbehörden können bei Fragen oder Beschwerden eingeschaltet werden. ■

Sinn und Zweck einer Sicherheitsüberprüfung

Die **Bundesbeauftragte** für den Datenschutz und die Informationsfreiheit stellt hierzu umfassende Informationen bereit. Diese sind abrufbar unter:

[Sinn und Zweck Info](#)





Und darf ich Ihren
Personalausweis sehen?

Zulässig? Ohne Zustimmung ist das Kopieren eines Personalausweises unzulässig.

Weil Kopien können missbräuchlich verwendet werden, etwa beim Identitätsdiebstahl oder bei Betrugsversuchen!

■ Personalausweis kopieren – oft gemacht, aber erlaubt?

Sie mieten ein Hotelzimmer oder ein Auto und werden gebeten, Ihren Personalausweis vorzulegen. Dabei stellen Sie fest, dass der Ausweis kopiert wird. Ist das zulässig? Und welche Regeln gelten in solchen Fällen?

Namen können eine Herausforderung sein

Selbst bei gebräuchlichen deutschen Namen kann es zu Unsicherheiten kommen. Schreibt sich jemand „Maier“, „Mair“ oder „Mayr“? Noch komplexer wird es bei ausländischen Namen.

Fehler bei der Schreibweise können dazu führen, dass Rechnungen nicht korrekt ausgestellt werden oder es im Einzelfall sogar zu Verwechslungen mit manchmal lustigen, oft aber peinlichen Folgen kommt. Vor diesem Hintergrund entsteht häufig die Idee, den Personalausweis einfach zu kopieren und die Kopie aufzubewahren. Was zunächst wie eine praktische Lösung erscheint, führt jedoch häufig zu datenschutzrechtlichen Problemen.

Gesetzliche Vorgaben zum Kopieren von Ausweisen

Das Personalausweisgesetz regelt in § 20 Absatz 2, dass Personalausweise nur mit Zustimmung der Ausweisinhaberin oder des Ausweisinhabers kopiert („abgelichtet“) werden dürfen. Der Begriff „ablichten“ ist bewusst weit gefasst und technikneutral. Er umfasst nicht nur klassische Kopien, sondern auch das Scannen oder Fotografieren eines Ausweises. Damit gilt grundsätzlich: Ohne Zustimmung ist das Kopieren eines Personalausweises unzulässig.

Warum diese Regelung sinnvoll ist

Die gesetzliche Vorgabe hat einen klaren Hintergrund. Ein Blick auf den Personalausweis zeigt: Er enthält deutlich mehr Informationen, als für eine Identifizierung erforderlich sind. Für die Feststellung der Identität reichen in der Regel Name, Vorname, Anschrift und Geburtsdatum.



Der Personalausweis enthält darüber hinaus weitere Angaben, etwa Geburtsort, Ausweisnummer, Größe und Augenfarbe. Diese zusätzlichen Informationen sind für viele Zwecke nicht erforderlich. Eine vollständige Kopie des Ausweises würde daher mehr Daten erfassen als nötig.

Das Aufschreiben der erforderlichen Angaben reicht aus

Der Personalausweis dient in erster Linie als Identitätsnachweis. Das hebt das Personalausweisgesetz in § 20 Absatz 1 ausdrücklich hervor. Dafür genügt es, dass der Ausweis vorgelegt wird und eine sogenannte Sichtprüfung erfolgt. Dabei wird das Lichtbild im Ausweis mit der Person abgeglichen. Wenn eine Dokumentation erforderlich ist, können die notwendigen Angaben erfasst und gespeichert werden. Eine Kopie des Ausweises ist dafür nicht erforderlich.

So ist es beispielsweise üblich und zulässig, dass ein Hotel die erforderlichen Daten eines Gastes erfasst oder eine Autovermietung Kundendaten dokumentiert. In beiden

Fällen reicht die Erfassung der notwendigen Informationen aus. Eine Kopie des Personalausweises ist hierfür grundsätzlich nicht erforderlich.

Es geht um das Vermeiden von Missbrauch

Die Anfertigung und Aufbewahrung von Ausweiskopien ist mit Risiken verbunden. Kopien können missbräuchlich verwendet werden, etwa beim Identitätsdiebstahl oder bei Betrugsversuchen. Auch wenn Unternehmen selbst kein missbräuchliches Interesse verfolgen, besteht stets das Risiko eines unbefugten Zugriffs, etwa durch Diebstahl oder unzureichende Sicherung. Grundsätzlich gilt daher: Daten, die nicht erhoben werden, können auch nicht missbraucht werden.

Es gibt aber gesetzliche Ausnahmen

In bestimmten Fällen sieht der Gesetzgeber ausdrücklich vor, dass Kopien von Personalausweisen zulässig oder sogar erforderlich sind.

Ein Beispiel ist das Geldwäschegesetz. Nach § 8 Absatz 2 sind Unternehmen in bestimmten Situationen verpflichtet, Ausweisdokumente zu kopieren oder zu erfassen. Dies betrifft unter anderem bestimmte Finanztransaktionen. So ist beispielsweise beim Kauf von Edelmetallen ab einem bestimmten Betrag eine Identitätsprüfung einschließlich Dokumentation vorgeschrieben. ■



Hotel

So ist es beispielsweise üblich und zulässig, dass ein Hotel die erforderlichen Daten eines Gastes erfasst oder eine Autovermietung Kundendaten dokumentiert. In beiden Fällen reicht die Erfassung der notwendigen Informationen aus. Eine Kopie des Personalausweises ist hierfür grundsätzlich nicht erforderlich.



Datenpannen
„helfen“
Internetkriminellen
gleich
mehrfach.

Sobald Angreifer
personenbezogene
Daten erbeuten, setzen
sie diese gezielt für
weitere Angriffe ein.

■ Gestohlene Daten: *Der Angriff endet nicht mit dem Hack*

Gelangen Daten von einer Hotelbuchungsplattform in falsche Hände, werden nicht nur die gebuchten Hotelaufenthalte sichtbar. Die Täter nutzen diese Daten aktiv weiter und starten zusätzliche Angriffe. Auf eine Datenpanne folgen so oft weitere Vorfälle.

Wenn Datenbanken von Hotels Sicherheitslücken haben

IT-Sicherheitsvorfälle und Cyberangriffe treten inzwischen regelmäßig auf und betreffen durch die zunehmende Digitalisierung nahezu jede Branche. Auch das Hotel- und Gaststättengewerbe nutzt das Internet seit langem intensiv. Hotelbuchungen erfolgen heute überwiegend online.

Nicht jeder Hotelbetrieb betreibt ein eigenes Buchungssystem. Deshalb greifen viele auf externe Plattformen zurück. Diese bündeln zahlreiche Angebote und verwalten entsprechend große Datenmengen. Durch die Vielzahl angeschlossener Hotels fallen enorme Mengen an Buchungen an. Entsprechend umfangreich sind die gespeicherten Kundendaten. Genau diese Daten machen die Plattformen zu attraktiven Zielen für Cyberkriminelle.

Wissen Sie, welche Folgen unsichere
Hotel-Plattformen haben können?

Wenn Cyberkriminelle eine Hotel-Plattform angreifen, sehen sie nur, wer welche Hotelzimmer gebucht hat – stimmt das? Nein. Hotel-Plattformen speichern in der Regel umfangreiche Kundendaten, nicht nur Buchungsinformationen. Ist die Datenbank unsicher und wird angegriffen, geraten daher vielfältige Daten der betroffenen Hotelkunden in Gefahr.

Können Täter im Namen der Kunden unerlaubt weitere Buchungen vornehmen?

Ja. Die Täter können die Daten auch für weitere Angriffe missbrauchen. Die Täter nutzen die erbeuteten Daten nicht nur für unerlaubte Buchungen, sondern auch für weitere Angriffe wie Phishing oder Betrug.

Datenschutzaufsichtsbehörden warnen vor weiteren Folgen

Angriffe auf Buchungsplattformen sind keine Theorie. So erhielt der **Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern** mehrfach Meldungen über Datenpannen bei Hotels, die eine verbreitete Buchungsdatenbank nutzen.

Die betroffenen Hotels wurden darüber informiert. In den abgeflissenen Daten befanden sich unter anderem Vor- und Nachnamen, Adressdaten sowie Buchungs- und Aufenthaltswahlungen.

Die Täter begannen schnell, diese Daten weiterzuverwenden. Sie versendeten beispielsweise Phishing-Nachrichten an Hotelkunden. Dabei gaben sie sich als Mitarbeitende der Hotels aus und versuchten, die Empfänger zu Zahlungen oder zur Herausgabe weiterer sensibler Daten zu bewegen.

Datenpannen „helfen“ Internetkriminellen gleich mehrfach

Dieses Beispiel zeigt deutlich: Sobald Angreifer personenbezogene Daten erbeuten, setzen sie diese gezielt für weitere Angriffe ein. Die Nutzungsmöglichkeiten sind vielfältig: gezielte Phishing-Angriffe, betrügerische Buchungen oder unberechtigte Abbuchungen.

Dabei beschränken sich die Täter nicht auf die ursprüngliche Plattform. Sie verwenden die Daten auch in anderen Zusammenhängen weiter. Mit den erlangten Informationen können sie gezielt Vertrauen ausnutzen und zusätzliche Schäden verursachen.

Das verdeutlicht, wie wichtig ein sorgfältiger Umgang mit personenbezogenen Daten ist. Unternehmen müssen Daten wirksam schützen und im Ernstfall schnell reagieren. Gleichzeitig hilft eine transparente Information der Betroffenen, weitere Schäden zu begrenzen, weil mögliche Folgeangriffe besser erkannt werden können. ■

Die Nutzungsmöglichkeiten sind vielfältig: gezielte Phishing-Angriffe, betrügerische Buchungen oder unberechtigte Abbuchungen.

