Newsletter Datenschutz
Ausgabe 12 | 2019

Konzept 17

Der Stand der Technik und die Folgen für den Datenschutz

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

Ihre neue Ausgabe macht es deutlich: Ob es um das Tragen von Namensschildern, um die Ortung von Firmenfahrzeugen, um Datenbrillen oder um 3D-Drucker im Unternehmen geht - immer können Menschen und ihre Privatsphäre betroffen sein. Der Datenschutz spielt in vielen Bereichen des beruflichen und privaten Lebens eine zentrale Rolle, auch wenn dies auf den ersten Blick nicht immer zu erkennen ist.

Das Themenspektrum im Datenschutz wird mit der dynamischen Entwicklung in der IT immer vielfältiger. Dabei muss der Datenschutz stets Schritt halten, sich also an den aktuellen Schutzbedarf und die neue Bedrohungslage anpassen und neue Technologien betrachten. Was die Forderung nach dem Stand der Technik für den Datenschutz genau bedeutet, erfahren Sie daher ebenfalls in dieser Ausgabe.

Ich wünsche Ihnen viel Spaß beim Lesen!
Ihr *Frank Berns, Datenschutzbeauftragter*

Pflicht zum Tragen von Namensschildern?

Kann der Arbeitgeber verlangen, dass Beschäftigte während der Arbeit Namensschilder tragen? Die Antwort lautet: Im Prinzip ja, aber es kommt doch sehr auf die konkreten Umstände an. Die berechtigten Interessen des Arbeitgebers sind genauso wichtig wie die berechtigten Interessen der Beschäftigten.

Funktionen eines Namensschilds

Ein Namensschild während der Arbeit kann in mehrfacher Hinsicht sinnvoll sein:

- Vor allem in größeren Unternehmen stellt es auf einen Blick klar, dass der Schildträger zum Unternehmen gehört. Konsequenterweise müssen Besucher oder Mitarbeiter von Fremdfirmen einen Besucherausweis oder einen Fremdfirmenausweis sichtbar tragen.
- Ein Namensschild erleichtert den Austausch unter Kollegen desselben Unternehmens. Das manchmal durchaus lästige Fragen nach dem Namen des anderen erübrigt sich.
- Bei Kundenkontakten entsteht durch ein Namensschild ein gewisser persönlicher Bezug zwischen Beschäftigtem und Kunde.

Unangenehme Erfahrungen - besonders von Frauen

Gerade der letzte Punkt zeigt aber, wie schnell ein Namensschild zu unangenehmen Erfahrungen führen kann. Vor allem Frauen wissen davon manchmal ein Lied zu singen. Das gilt besonders, wenn auf dem Namensschild sowohl der Vorname als auch der Nachname stehen. Mancher Kunde kann es sich nicht verkneifen, die Frau mit dem Vornamen anzusprechen. Und es kommt durchaus vor, dass ein Kunde dann ihre Hobbys und Ähnliches im Internet recherchiert.

Vorname: regelmäßig nicht erforderlich

Vornamen auf Namensschildern sind daher kritisch zu sehen. Im Regelfall sind sie nicht erforderlich. Das gilt auch, wenn der Nachname häufig ist. Das Argument, dann sei zur Unterscheidung zusätzlich der Vorname notwendig, hat kein Gewicht. Denn nicht selten sind auch die Vornamen identisch. Beispiel: Sandra Müller gibt es in jedem großen Unternehmen mehrfach. Außerdem schafft die dienstliche Telefonnummer rasch Klarheit.

Einwilligung: nur für den Vornamen nötig

Manchmal hört man die Behauptung, dass ein Namensschild nur zulässig sei, wenn der Beschäftigte eingewilligt hat. Das ist so nicht richtig. Die Datenschutz-Grundverordnung (DSGVO) erlaubt Namensschilder auch ohne Einwilligung des Beschäftigten, wenn der Arbeitgeber an solchen Schildern ein berechtigtes Interesse hat. Das ist aus den Gründen, die schon genannt wurden, normalerweise der Fall.

Aber wohlgemerkt: Das bezieht sich nur auf Schilder mit dem Nachnamen. Was den Vornamen angeht, überwiegen im Normalfall die Interessen des Beschäftigten. Die Folge: Auch den Vornamen auf dem Schild anzugeben, wäre nur zulässig, wenn der Beschäftigte damit einverstanden ist.

Betriebsvereinbarungen sind möglich

In Unternehmen mit Betriebsrat gibt es manchmal Betriebsvereinbarungen zum Thema Namensschilder. Falls eine solche Betriebsvereinbarung existiert, sind ihre Bestimmungen maßgeblich.

Anwendbarkeit der DSGVO

Nur für Fachleute interessant ist die Frage, ob die DSGVO für Namensschilder von Beschäftigten überhaupt gilt. Der Grund: Selbst wenn sie nicht gelten würde, müsste man immer die Interessen beider Seiten berücksichtigen - also sowohl die Interessen des Arbeitnehmers als auch die Interessen der Beschäftigten.

Kontakt zu uns: mail@konzept17.de

GPS-Überwachung von Firmenfahrzeugen?

Rein technisch gesehen geht bei der Überwachung von Firmenfahrzeugen fast alles. Und vieles davon ist rechtlich erlaubt. Aber es gibt auch Grenzen. Lesen Sie, wo die roten Linien verlaufen.

Unterschiedliche Fahrzeugarten

Unternehmen setzen Fahrzeuge ganz unterschiedlicher Art ein. Das reicht von Kundendienstfahrzeugen über Transportfahrzeuge bis hin zu "Vertreterfahrzeugen" für Außendienstmitarbeiter. Ortungssysteme, die GPS verwenden, lassen sich im Prinzip bei allen Arten von Fahrzeugen einbauen. Trotzdem macht es rechtlich gesehen einen Unterschied, um welche Art von Fahrzeugen es geht. Beispiel: Der Schutz gegen den Diebstahl von Ladung kann bei Transportfahrzeugen sehr wichtig sein. Bei einem Vertreterfahrzeug spielt er dagegen normalerweise keine Rolle.

Erforderlichkeit als Schlüsselbegriff

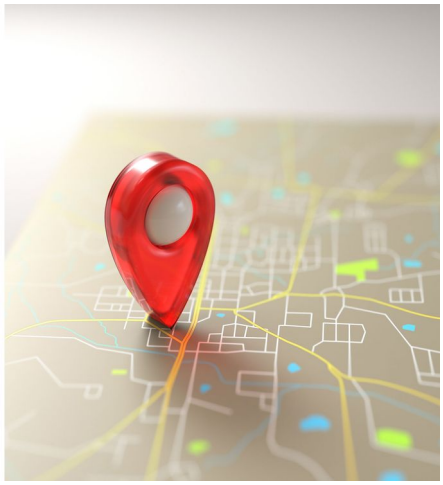
Solche Überlegungen führen zum entscheidenden Punkt: Für den Einsatz von Ortungssystemen ist eine Begründung notwendig. Die Art und Weise, wie das System eingesetzt wird, muss erforderlich sein. "Einfach so" dürfen Unternehmen ihre Fahrzeuge nicht mit Ortungssystemen ausstatten.

Speicherung oder nicht?

Es macht auch einen gewaltigen Unterschied, ob die Ortungsdaten gespeichert werden oder nicht. Werden sie gespeichert, stellt sich die Frage, wozu das geschieht. Es muss also feststehen, was der Zweck der Speicherung ist. Dabei muss es um einen Zweck gehen, der rechtlich akzeptabel ist. Und die Speicherung muss für diesen Zweck erforderlich sein.

Kontrolle des Verhaltens - ein heikler Punkt

Schnell heikel wird es dann, wenn gespeicherte Ortungsdaten es erlauben, das Verhalten des Fahrers zu kontrollieren. Konkretes Beispiel: Ein Fahrzeug transportiert sehr wertvolle Maschinen. Verständlich, dass das Unternehmen stets wissen will, wo sich das Fahrzeug gerade befindet. Das heißt aber auch, dass jede Toilettenpause des Fahrers registriert wird. Dann stellt sich die Frage, ob der Arbeitgeber ihm vielleicht vorhalten darf, dass er zu viele solche Pausen macht. Denkbar wäre dann zum Beispiel, dass der Arbeitgeber auf derartige Vorhaltungen von vornherein ausdrücklich verzichtet.



Wo ist der LKW mit der wertvollen Ladung?

Entscheidende Details

Das alles ist im Prinzip nicht neu und hat sich auch durch die Datenschutz-Grundverordnung nicht geändert. Der Teufel steckt jedoch wie so oft im Detail. Über das Grundsätzliche ist man sich schnell einig. Wenn es um die Einzelheiten geht, kann das durchaus anders aussehen. Es wundert deshalb nicht, dass sich sowohl die Gerichte als auch die Aufsichtsbehörden für den Datenschutz schon öfter mit dem Thema befasst haben. Dabei ergeben sich interessante Aufschlüsse.

Beispiel: Daten für ein Fahrtenbuch

Sehr kritisch gehen Aufsichtsbehörden für den Datenschutz mit dem Argument um, Ortungsdaten müssten gespeichert werden, um ein ordnungsgemäßes Fahrtenbuch zu führen. Sie halten dieses Argument für zu pauschal. Sie haben bei Finanzämtern und Straßenverkehrsbehörden nachgefragt, welche Daten diese Ämter für ein Fahrtenbuch fordern. Üblicherweise reichen danach folgende Angaben aus: Datum, Start- und Endpunkt der Fahrt, gefahrene Kilometer, Kilometerstand, Fahrtzweck. Damit sind jedenfalls für den Zweck "Fahrtenbuch" nur diese Daten erforderlich, andere Daten dagegen nicht.

Beispiel: Daten für die Fahrzeugdisposition

Deutlich offener sind die Aufsichtsbehörden für das Argument, Ortungsdaten seien für die Fahrzeugdisposition notwendig. Klassisches Beispiel: Bei einem Stau muss eine Spedition ihren Kunden darüber informieren können, wie stark sich die Ankunft verzögert. Anders wären beispielsweise Just-in-Time-Anlieferungen für Produktionsbetriebe nicht sinnvoll möglich. Eine längere Speicherung der Ortungsdaten ist für diesen Zweck allerdings im Normalfall nicht erforderlich.

Beispiel: Streit um die pünktliche Anlieferung

Gerade dieses Beispiel zeigt aber, wie genau man hinsehen muss. Wenn der Kunde einer Spedition eine verspätete Lieferung reklamiert, muss die Spedition natürlich nachvollziehen können, ob der Kunde Recht hat. Das geht nicht, ohne die Ankunftsdaten der Lieferung zumindest so lange zu speichern, wie eine Reklamation möglich ist.

Beispiel: Bezahlung nach der Einsatzzeit

Manchmal müssen Kunden den Einsatz von Fahrzeugen nach Zeit bezahlen. Das ist zum Beispiel für Kranfahrzeuge üblich, aber auch für sonstige Spezialfahrzeuge. Eine ordnungsgemäße Abrechnung ist dann nur möglich, wenn die dafür notwendigen Daten gespeichert sind. Sobald die Abrechnung einvernehmlich abgeschlossen ist, entfällt aber die Erforderlichkeit der Speicherung. Dann sind die Daten zu löschen.

Miteinander reden - Argumente austauschen!

Die verschiedenen Beispiele zeigen vor allem eines: Ein pauschales Vorgehen ist nicht möglich. Wenn es unterschiedliche Meinungen zum Thema "Erforderlichkeit" gibt, sollte man deshalb im Unternehmen miteinander sprechen und die Argumente austauschen.

Impressum

Redaktion:
Frank Berns
Datenschutzbeauftragter

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de

Der Stand der Technik und die Folgen für den Datenschutz

Führen Unternehmen neue Sicherheitsverfahren ein, entsteht meistens ein Aufwand durch Schulung und Umgewöhnung. Doch der Wechsel hat seinen Sinn: Der Stand der Technik ändert sich, die Datensicherheit muss sich anpassen.

Schon wieder eine neue Verschlüsselungslösung ...

Obwohl es für den Datenschutz so wichtig ist, kommt die Verschlüsselung vertraulicher Daten in vielen Unternehmen nicht voran. Ein häufig genannter Grund dafür ist, dass die Beschäftigten die Anwendung der Verschlüsselungslösungen als zu kompliziert und umständlich empfinden.

Erschwerend kommt hinzu: Hat man sich gerade an eine Verschlüsselungslösung gewöhnt, kommt eine Produktänderung, oder das Unternehmen führt ein völlig neues Produkt zur Verschlüsselung ein. Es folgen neue Schulungen, als Nutzer muss man sich umgewöhnen.

Warum werden überhaupt neue Lösungen für die Datensicherheit eingeführt? Waren die bisherigen doch nicht so gut?

IT-Sicherheit unterliegt ständigem Wandel

Auch wenn die bisherige IT-Sicherheitslösung früher gut geschützt haben mag: Die Risiken für personenbezogene Daten, die Methoden der Datenspione und die zu schützenden IT-Verfahren verändern sich in rascher Folge. Unternehmen und Behörden müssen die Sicherheitsverfahren an die sich ändernde Bedrohungslage und den jeweils aktuellen Schutzbedarf der Daten anpassen.

BSI-Richtlinien

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig Technische Richtlinien, die zum Beispiel Empfehlungen für Verschlüsselungsverfahren enthalten, die für einen bestimmten Zeitraum als sicher eingestuft werden. Stellt sich heraus, dass sich ein Verschlüsselungsverfahren doch knacken lässt, dass es also unsicher ist, passt das BSI die Richtlinien umgehend an.

Entsprechend müssen auch die Anbieter ihre IT-Sicherheitslösungen überarbeiten, verändern oder neu herausbringen. Und entsprechend müssen Unternehmen reagieren.

Datenschutzrecht fordert Stand der Technik

Die Datenschutz-Grundverordnung (DSGVO) fordert deshalb auch ausdrücklich technische und organisatorische Maßnahmen, um die Datensicherheit zu gewährleisten. Diese Maßnahmen müssen insbesondere unter Berücksichtigung des Stands der Technik ausgewählt werden. Hier ist also die Unternehmensleistung ständig gefragt, sich über den Stand der Technik zu informieren und die Maßnahmen für die Datensicherheit aktuell zu halten.

Unter "Stand der Technik" versteht man, dass die gewählten Schutzmaßnahmen das gegenwärtig realisierbare Sicherheitsniveau erreichen müssen, das auf dem aktuellen Lösungsmarkt den Standard bildet. Sicherheitsmaßnahmen, die auf dem Markt als überholt und veraltet eingestuft werden, entsprechen nicht dieser Vorgabe.

Auch der Arbeitsschutz zum Beispiel fordert den Stand der Technik ein als "Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Gesundheit und zur Sicherheit der Beschäftigten gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt worden sind."

Was als sichere Verschlüsselung gilt, ändert sich immer wieder

Als Anwenderin oder Anwender der IT-Sicherheitslösungen ist man ebenfalls diesem Stand der Technik unterworfen, man muss die neuen Lösungen erlernen. Das ist zweifellos Aufwand. Doch ohne Datensicherheit nach dem Stand der Technik lassen sich die personenbezogenen Daten nicht angemessen schützen. Datenschutz und Stand der Technik gehören also zwingend zusammen.

Auch Passwortrichtlinie muss aktuell gehalten werden

Es sind aber nicht nur die technischen Lösungen, die dem Stand der Technik entsprechen müssen. Die Datenschutz-Grundverordnung fordert auch für organisatorische Maßnahmen, dass sie den Stand der Technik einhalten. Das betrifft zum Beispiel die Wahl eines sicheren Passworts, wie es eine Passwortrichtlinie vorgeben sollte.

Was als sicheres Passwort gilt, ändert sich mit der Zeit, wobei die nötige Stärke und Komplexität für Passwörter stetig zunehmen. So fordert zum Beispiel der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Baden-Württemberg starke Passwörter, die aus zwölf oder mehr Zeichen bestehen. Je wichtiger das Passwort ist, desto länger sollte es sein. Passwörter sollten sowohl Klein- als auch Großbuchstaben, Ziffern und Satzzeichen enthalten.

Früher wurden auch Passwörter mit weniger Zeichen als sicher und stark genug eingestuft. Doch die Zeiten ändern sich und damit die Bedrohungslage für den Datenschutz sowie der Stand der Technik. Inzwischen verfügen Datendiebe über Rechenkapazitäten und Angriffsverfahren, die mehrere Milliarden Passwörter pro Sekunde ausprobieren können. Daher ist es essenziell, stärkere Passwörter zu verwenden als früher. Nur so ist Angreifern effektiv beizukommen, die sich geknackte Passwörter zunutze machen.

Was haben 3D-Druck und Smart Glasses mit dem Datenschutz zu tun?

Kaum kommt eine neue Technologie auf den Markt, schon wird auf Risiken für den Datenschutz hingewiesen. Dabei scheinen 3D-Druck oder Smart Glasses doch harmlos zu sein, oder etwa nicht? Leider kann das Gegenteil der Fall sein!

Datenschutz ist keine "Spaßbremse"

Man muss kein sogenannter Nerd sein, um an neuen technischen Lösungen Freude zu haben. Es ist schon faszinierend, was man mit einem 3D-Drucker erzeugen kann oder welche Möglichkeiten sich bei der Nutzung einer Datenbrille (Smart Glasses) auftun. Es gibt sogar Anwendungsbereiche für solche neuen Technologien, die sehr viel Gutes erhoffen lassen, zum Beispiel in der Medizin.

Doch der Datenschutz sieht solche neuen Technologien scheinbar immer kritisch. Dabei wollen Datenschützer niemandem den Spaß verderben oder gar wichtige Entwicklungen behindern. Was der Datenschutz aber vorsieht, ist die Prüfung, welche Folgen und Risiken entstehen, wenn neue Technologien eingeführt und genutzt werden.

Smart Glasses und die Datenschutzfolgen

Betrachtet man zum Beispiel Smart Glasses, stellt man fest: Smart Glasses haben mit klassischen Brillen wenig zu tun. In der Regel sind sie überhaupt keine Sehhilfe im Sinne einer Brille. Vielmehr handelt es sich um etwas wie ein Smartphone, das man auf der Nase trägt, um es einmal bildlich zu sagen.

Smart Glasses werden aus gutem Grund auch als Datenbrillen bezeichnet. Sie reichern das visuelle Bild durch zusätzliche Informationen an, sie können auch Daten erheben und an Cloud-Dienste übertragen. Das können Gesichtsbilder, Videos und Tonaufnahmen von Personen sein, die sich in ihrer Reichweite befinden. Es gibt bereits Anwendungen für Smart Glasses, um Personen im Blickfeld mithilfe von Gesichts- und Spracherkennung zu identifizieren. Offensichtlich wird hier der Datenschutz berührt.

3D-Drucker und die Datenschutzfolgen

Ein weiteres Beispiel für neue Technologien, die mehr mit dem Datenschutz zu tun haben, als man zuerst denken mag, sind 3D-Drucker. Das Besondere eines 3D-Druckers ist es, dass sich damit individuelle Produkte erzeugen lassen; im medizinischen Bereich individuell für eine spezielle Person. Hier ist die Verbindung zum Datenschutz offensichtlich.

Wie herkömmliche Drucker auch speichern 3D-Drucker die Daten, die zu einem Druckauftrag gehören. Da gerade im 3D-Druck die Erzeugnisse sehr vom einzelnen Kunden abhängen können, ist es sehr wahrscheinlich, dass der Druckauftrag an den 3D-Drucker Kundendaten enthält.

Bei neuen Technologien immer auch an den Datenschutz denken

Diese Beispiele machen deutlich: Sollen neue Technologien wie Datenbrillen, 3D-Drucker oder andere neue Verfahren zum Einsatz kommen, sollte man nicht nur von den vielen neuen Möglichkeiten und Chancen angetan sein, sondern auch immer an die möglichen Folgen für den Datenschutz denken.

Kaum eine technische Lösung, die uns begeistert, hat nichts mit uns Menschen zu tun. In den meisten Fällen betreffen neue Technologien den Menschen und auch die Privatsphäre des Menschen. Deshalb ist es gut und richtig, wenn Datenschützer sofort bei neuen Entwicklungen auf die möglichen Risiken hinweisen. Letztlich müssen auch Unternehmen die Risiken sehen, sie analysieren und sie soweit wie möglich minimieren. Denn die Datenschutz-Grundverordnung (DSGVO) sieht bei neuen Technologien eine sogenannte Datenschutz-Folgenabschätzung vor.

Nur wenn man die Risiken kennt und bewerten kann, ist man in der Lage, sie abzuwenden. Und nur dann machen neue Technologien wirklich Spaß. Der Datenschutz ist also keine Spaßbremse, sondern hilft, neue Techniken sicher umzusetzen.

Sehen Sie die möglichen Risiken neuer Technologien? Machen Sie den Test!

Frage: Smart Glasses ergänzen Daten zum visuellen Bild, aber sie erheben keine Daten. Stimmt das?

a) Nein, Datenbrillen können auch Daten wie etwa Fotos und Videos aufzeichnen und an eine Cloud übertragen.
b) Ja, denn das ist ja nicht der Zweck einer Datenbrille, sie soll nur Zusatzinformationen zum Bild liefern, mehr nicht.

Lösung: Die Antwort a) ist richtig, auch wenn ein Unternehmen eine Datenbrille nicht so einsetzen will, dass Personen im Blickfeld des Nutzers aufgezeichnet und die personenbezogenen Daten ausgewertet werden. Besteht eine technische Option, muss man auch daran denken, dass jemand diese Option nutzen könnte. Dann gilt es, die unerwünschte Anwendung zu verhindern.

Frage: 3D-Drucker erzeugen meistens Bauteile, mit Personen hat dies nichts zu tun. Stimmt das?

a) Ja, denn 3D-Drucker werden besonders in der Fertigungsindustrie eingesetzt.
b) Nein, 3D-Drucker können sowohl im medizinischen Bereich für Menschen eingesetzt werden als auch Kundendaten verarbeiten.

Lösung: Die Antwort b) ist richtig. 3D-Drucker erzeugen individuelle Produkte, für einen bestimmten Kunden oder für einen bestimmten Patienten. Deshalb werden entweder personenbezogene Daten direkt verarbeitet, oder sie sind mit dem Druckauftrag verknüpft. Der 3D-Drucker speichert sie zwischen und Unbefugte könnten sie abgreifen. Deshalb sind 3D-Drucker durchaus ein Thema für den Datenschutz.