HANSMEYER § CONSULT
DATENSCHUTZ · PERSONAL

Datenschutz *Beratungsbrief!*

Christina Hansmeyer Datenschutz - Information

Liebe Leserin, lieber Leser,

dürfen die personenbezogenen Daten verarbeitet werden oder nicht? Auf diese Grundfrage des Datenschutzes können Sie in ganz unterschiedlichen Situationen treffen: Ihr Arbeitgeber möchte z.B. Ihren Führerschein kopieren. Müssen Sie zuerst einwilligen? Das beantwortet die neue Ausgabe ebenso wie die Frage, wann die Verwendung von Videobeweisen bei Verkehrsstraftaten zulässig ist.

Manchmal geben Sie vielleicht Ihre Einwilligung zur Nutzung Ihrer personenbezogenen Daten, ohne dies wirklich zu wissen. Information und Transparenz sind im Datenschutz aber entscheidend. Deshalb zeigt Ihnen diese Ausgabe, worauf Sie in puncto Einstellungen bei Windows 10 und bei der Freigabe von Dokumenten unter Office 365 achten sollten.

Ich wünsche Ihnen wieder eine spannende Lektüre!
Herzlichst Ihre Christina Hansmeyer

Darf der Arbeitgeber meinen Führerschein kopieren?

Viele Arbeitnehmer fahren Firmenfahrzeuge, weil sie ihre Arbeit anders gar nicht erledigen könnten. Darf der Arbeitgeber in solchen Fällen den Führerschein des Mitarbeiters kopieren, um im Ernstfall nachweisen zu können, dass dieser ihm tatsächlich die erforderliche Fahrerlaubnis nachgewiesen hatte?

Aller Anlass zur Vorsicht für den Arbeitgeber

Wenn ein Arbeitgeber zulässt, dass ein Arbeitnehmer ein Firmenfahrzeug führt, obwohl dieser nicht über die erforderliche Fahrerlaubnis verfügt, riskiert der Arbeitgeber eine Freiheitsstrafe bis zu einem Jahr. Das ergibt sich aus § 21 Abs. 1 Nr. 2 Straßenverkehrsgesetz. Außerdem droht in einem solchen Fall bei Unfällen erheblicher Ärger vor allem mit der Kaskoversicherung. In aller Regel wird die Versicherung nämlich jede Leistung verweigern. Es ist daher verständlich, dass Arbeitgeber sich gegen ein solches Risiko absichern wollen.

Aber was folgt daraus?

Immer wieder wird darüber gestritten, welche Maßnahmen dabei zulässig und angemessen sind. Reicht es aus, dass der Arbeitgeber oder eine von ihm beauftragte Person (zum Beispiel ein Fuhrparkleiter) sich den Führerschein des Arbeitnehmers vorlegen lässt und eine kurze Notiz darüber anfertigt, dass die erforderliche Fahrerlaubnis vorhanden war? Oder ist der Arbeitgeber berechtigt, den Führerschein des Mitarbeiters zu kopieren und diese Kopie aufzubewahren?

Hat der Fahrer eines Firmenfahrzeugs keinen Führerschein, gibt es im Ernstfall Probleme zum Beispiel mit der Versicherung
(Bild: AzmanJaka/iStock/Thinkstock)

Klare Position aus Bayern

Das Bayerische Landesamt für Datenschutzaufsicht als Spezialbehörde für den Datenschutz in der Privatwirtschaft hat dazu klar Stellung bezogen: Der Arbeitgeber darf in solchen Fällen den Führerschein kopieren! Eine solche Kopie sei - so das Hauptargument des Landesamts für Datenschutz - für den Arbeitgeber hilfreich, wenn er nachweisen müsse, dass die notwendige Fahrerlaubnis vorhanden gewesen sei.

Kopie durch den Arbeitgeber ist zulässig!

Datenschutzrechtliche Bedenken sieht das Landesamt nicht. Die Anfertigung einer Kopie ist nach seiner Auffassung für die Durchführung des Beschäftigungsverhältnisses erforderlich. Die Voraussetzungen des insoweit einschlägigen § 32 Abs. 1 Satz 1 des Bundesdatenschutzgesetzes, der den Datenschutz im Beschäftigungsverhältnis regelt, seien daher gegeben. Der Arbeitgeber dürfe eine Kopie des Führerscheins anfertigen und aufbewahren.

Es geht um banale Daten

Kritikern dieser Auffassung entgegnet das Landesamt, dass ein Führerschein lediglich Daten enthalte, die dem Arbeitgeber ohnehin schon bekannt seien (etwa Name und Vorname) oder die als eher banal einzustufen seien (etwa die Führerscheinklasse).

Windows 10: Datenschutzeinstellungen nicht vergessen!

Das neue Microsoft-Betriebssystem zeigt deutlich, wie wichtig die Datenschutzkontrolle ist, bevor man neue Software nutzt. Denn Datenschutz als Standard ist auf dem IT-Markt bisher kaum in Sicht.

Ein verlockendes Angebot?

Windows 10 erfreute sich gleich nach seinem Start Ende Juli 2015 großer Beliebtheit bei den Nutzern. Einer der Gründe dürfte sein, dass das Betriebssystem unter bestimmten Bedingungen als kostenloses Upgrade erhältlich ist. Doch kaum war das neue Betriebssystem von Microsoft auf dem Markt, meldeten sich Daten- und Verbraucherschützer mit deutlicher Kritik zu Wort. So bezeichnete der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit Windows 10 als "Fenster zur Privatsphäre". Die Verbraucherzentrale Rheinland-Pfalz e.V. sprach bei Windows 10 von "Überwachung bis zum letzten Klick".

Datenschutzerklärungen bleiben oft ungelesen

Die Medien haben daraufhin viel über den Datenschutz bei Windows 10 berichtet. Viele Nutzer waren überrascht von den Meldungen über die Sammlung personenbezogener Daten durch das Betriebssystem. Hätte man allerdings die Datenschutzbestimmungen von Windows 10 gelesen, wäre die Überraschung geringer gewesen. Denn dort liest man, dass Windows 10 eine "personalisierte IT-Umgebung" ist und dass die Schlüsselkomponenten von Windows auf der Cloud beruhen. Weiter heißt es dort: "Um dieses Computer-Erlebnis anzubieten, erheben wir Daten über Sie, Ihr Gerät und wie Sie Windows verwenden. Und weil Windows für Sie persönlich ist, geben wir Ihnen die Wahlmöglichkeiten darüber, welche personenbezogenen Daten wir sammeln und wie wir diese verwenden dürfen."

Datenschutz-Optionen müssen auch genutzt werden

Tatsächlich informiert Microsoft also über die Sammlung personenbezogener Daten. Manche Datenschützer lobten deshalb die Transparenz bei Windows 10. Was allerdings nicht den Vorstellungen des Datenschutzes entspricht, ist die im IT-Markt weit verbreitete Vorgehensweise, die Datenschutzeinstellungen im Standard eher datenschutzunfreundlich zu gestalten.

Windows 10 lockt mit zum Teil kostenlosem Upgrade - doch ohne angepasste Datenschutz-Einstellungen sammelt es zahlreiche persönliche Daten
(Bild: Imilian/iStock/Thinkstock)

"Datenschutz als Standard" oder "Privacy by Design" hat also noch eher Seltenheitswert. Für Unternehmen und jeden einzelnen Nutzer von Windows 10 bedeutet das, die Datenschutz-Optionen zu überprüfen und individuell einzustellen.

Bequemlichkeit kann riskant sein

Die größte Gefahr bei Datenschutz-Optionen ist, dass man als Nutzer die Voreinstellungen ungeprüft übernimmt und damit die Entscheidung über den anzuwendenden Datenschutz dem jeweiligen Anbieter überlässt. Das gilt nicht nur für Microsoft und Windows 10, sondern ganz generell. Im Fall von Windows 10 sollte man also nicht die "Express-Einstellungen" bei der Installation wählen, sondern sich die Zeit nehmen, die vielfältigen Einstellungsmöglichkeiten rund um den Datenschutz zu sichten und zu nutzen. Abkürzungen wie die "Express-Einstellungen" erscheinen komfortabel und bequem. Doch sie sind nicht ohne Weiteres zu empfehlen.

Viele Einstellungen haben Bezug zum Datenschutz

Wer sich die Funktion "Einstellungen" bei Windows 10 ansieht, findet dort auch spezielle Datenschutzoptionen. Im Prinzip können sich aber auch in vielen anderen Auswahlbereichen Einstellungen finden, die für den Datenschutz wichtig sind. Bei Windows 10 sind das zum Beispiel neben "Datenschutz" auch Einstelloptionen wie "System", "Geräte", "Netzwerk und Internet", "Personalisierung", "Konten", "Zeit und Sprache" sowie "Update und Sicherheit".

Unter den "Datenschutzeinstellungen" bei Windows 10 finden sich dann gebündelte Auswahloptionen, die Sie allesamt durchsehen sollten. Nicht immer ist direkt ersichtlich und verständlich, warum dieser oder jener Punkt Relevanz für den Datenschutz haben könnte. Doch Einstellungen zum Beispiel zur Kamera legen fest, welche Anwendungen die Bilder nutzen dürfen. Würde es hier keine Einschränkung geben, könnten Bilder an Anwendungen und Dritte gelangen, die diese eigentlich nicht bekommen sollten, würde man den betroffenen Nutzer konkret fragen.

Datenschutz kann Verzicht mit sich bringen

Je nach Option führt die datenschutzfreundliche Einstellung allerdings dazu, dass sich bestimmte Funktionen nicht mehr vollständig oder sogar überhaupt nicht mehr nutzen lassen. Die Spracherkennung Cortana zum Beispiel möchte für eine vollständige Funktion auch Zugriff auf Standortdaten, E-Mails, SMS, Kontaktdaten, Suchverlauf des Browsers und Kalendereinträge. Unterbindet man bestimmte Zugriffe, sind die Funktionen des Sprachassistenten eingeschränkt. Wenn man die Weitergabe der Standortdaten nicht zulässt, funktioniert der digitale Assistent Cortana überhaupt nicht. Das ist bedauerlich. Denn viele Spracheingabe-Funktionen brauchen eigentlich keine aktuellen Positionsdaten.

Der Datenschutz sollte es Ihnen aber wert sein, auf bestimmte Funktionen zu verzichten, insbesondere dann, wenn Datenzugriffe, die die Software fordert, aus Nutzersicht nicht nachvollziehbar sind. Grundsätzlich sollten Datenschutzerklärung und Datenschutzeinstellungen weitaus mehr Beachtung finden - und zwar nicht nur bei Windows 10, sondern bei jeder Software und bei jedem Online-Service.

Impressum/ Redaktion:

Christina Hansmeyer
Externe Datenschutzbeauftragte, Juristin

Hansmeyer Consult
Kanzlei für Datenschutz & Datensicherheit

Samlandweg 19
33719 Bielefeld
Tel.: +49 (521) 38 33 784
E-Mail: info@hansmeyerconsult.de
www.hansmeyerconsult.de

Zur Ansicht und Anwendung empfohlen:
www.neuland-medien.de
Kooperationspartner von Hansmeyer Consult

Dash-Cam-Aufnahmen im Strafprozess - ein zulässiges Beweismittel?

Bei Schadensersatzprozessen nach einem Verkehrsunfall werden Aufnahmen von Dash-Cams, also von Kameras, die an der Windschutzscheibe angebracht sind, nicht als Beweismittel anerkannt. Das ist inzwischen allgemeine Meinung. Aber wie sieht es in einem Strafverfahren aus? Vor allem dann, wenn das Opfer buchstäblich einen Unfall kommen sah und deshalb kurz vor dem befürchteten Crash die Kamera einschaltete? Lässt sich auf solche Aufnahmen eine Verurteilung stützen?

Wahnsinn auf der Autobahn

Im Straßenverkehr kommen manchmal Situationen vor, die selbst der fantasievollste Drehbuchautor nicht erfinden könnte. Davon kann ein Autofahrer ein Lied singen, der sonntagabends mit etwa 100 km/h auf der rechten Fahrspur einer deutschen Autobahn fuhr. Er sagte als Zeuge vor Gericht Folgendes aus:

Der Angeklagte überholte ihn zunächst links mit einer geringfügig höheren Geschwindigkeit. Als sich der spätere Angeklagte etwas mehr als eine Fahrzeuglänge vor das Fahrzeug des Zeugen geschoben hatte, wechselte er bei freier Bahn und ohne zu blinken von der linken auf die rechte Spur. Dort verlangsamte er seine Geschwindigkeit. Dies hatte zur Folge, dass sich der Abstand zwischen den beiden Fahrzeugen sofort auf weniger als eine Fahrzeuglänge verringerte.

Mit diesem wahnwitzigen Fahrmanöver wollte der Angeklagte den Zeugen zum Abbremsen oder Ausweichen veranlassen, um ihn so für ein angeblich verkehrswidriges Verhalten zu maßregeln.

Nur mit viel Glück kam es zu keinem schweren Unfall

Nur mit größter Mühe konnte der Zeuge einen Auffahrunfall verhindern. Dazu wechselte er auf den linken Fahrstreifen und überholte das Fahrzeug des Angeklagten. Noch während der Zeuge sein Fahrzeug beschleunigte, driftete das Fahrzeug des Angeklagten über die Mittelmarkierung. Deshalb musste der Zeuge noch weiter nach links hin zur Mittelleitplanke ausweichen.

Als sich die beiden Fahrzeuge auf gleicher Höhe befanden, betrug der Seitenabstand zwischen ihnen bei einer Geschwindigkeit von rund 100 km/h nur noch ungefähr 5 cm. Nur durch Zufall kam es nicht zu einem schweren Verkehrsunfall.

Einziger Beweis: Aufnahmen einer Dash-Cam

Diese Vorfälle stehen nur deshalb fest, weil der Zeuge Aufnahmen mit einer Dash-Cam angefertigt hat. Ihm war das Fahrzeug des Angeklagten nämlich kurz zuvor durch sehr dichtes Auffahren aufgefallen. Um für den Fall eines möglichen Zusammenstoßes Beweise in der Hand zu haben, aktivierte der Zeuge sofort die Kamera, die neben seinem Innenspiegel angebracht war. Diese Aufnahmen verwendete die Staatsanwaltschaft nun als Beweismittel im Strafverfahren.

Strafe: Acht Monate auf Bewährung

Tatsächlich wurde der Angeklagte auf dieser Basis vom Amtsgericht Nienburg am 20. Januar 2015 auch verurteilt, und zwar zu einer Freiheitsstrafe von acht Monaten auf Bewährung. Außerdem wurde ihm die Fahrerlaubnis entzogen.

Zwei unterschiedliche Fragen

Da das Gericht die Verurteilung wesentlich auf die Auswertung der Filmaufnahmen stützte, musste es auch dazu Stellung nehmen, ob diese Aufnahmen überhaupt als Beweismittel verwendet werden dürfen. Zur teils erheblichen Überraschung von Datenschützern hat es diese Frage bejaht.

Die Aufnahmen einer Dash-Cam hinter der Windschutzscheibe lassen sich unter Umständen doch als Beweise in einem Prozess verwenden
(Bild: vsurkov/iStock/Thinkstock)

Dabei unterscheidet es zwei Aspekte:

- War der Zeuge dazu berechtigt, die Aufnahmen anzufertigen?
- Dürfen die Aufnahmen als Beweismittel verwendet werden?

Recht zum Anfertigen der Aufnahmen

Zunächst wendet sich das Gericht der Frage zu, ob der Zeuge dazu berechtigt war, Aufnahmen anzufertigen. In diesem speziellen Fall ist diese Frage nach Auffassung des Gerichts zu bejahen. Das Interesse des Zeugen an Aufnahmen zur Beweissicherung überwiege das Interesse des Angeklagten an der Unverletzlichkeit seines Rechts auf informationelle Selbstbestimmung. Dies ergebe sich daraus, dass wegen des dichten Auffahrens ein nachvollziehbarer Anlass vorhanden gewesen sei, einen Unfall zu fürchten. Deshalb habe der Zeuge ein berechtigtes Interesse daran gehabt, Beweise zu sichern.

Verwendung der Aufnahmen als Beweismittel

Ausgehend davon gelangt das Gericht zu dem Schluss, dass auch die zweite Frage zu bejahen ist: Die Aufnahmen dürfen als Beweismittel verwendet werden! Dafür führt es gleich mehrere Argumente an.

- Zum einen sei es so, dass die Aufnahmen Vorgänge aus dem öffentlichen Straßenverkehr betreffen und dass der Kernbereich der persönlichen Lebensführung deshalb nicht berührt werde.
- Außerdem sei zu berücksichtigen, dass nicht der Angeklagte selbst, sondern nur sein Fahrzeug auf den Aufnahmen zu sehen ist.
- Und schließlich sei es auch nicht so, dass sich der Zeuge zu einer Art Hilfssheriff aufgeschwungen hätte. Vielmehr habe für ihn wegen des dichten Auffahrens ein konkreter Anlass für die Aufnahmen bestanden.

Ein schlichter, aber guter Rat: regelkonform fahren!

Der Fall zeigt, dass die Aussage "Aufnahmen mit Dash-Cams sind keine zulässigen Beweismittel" in dieser generellen Form nicht zutrifft. Am besten wäre es freilich, es gar nicht so weit kommen zu lassen, dass über diese Aussage nachgedacht werden muss, und sich stattdessen an die Verkehrsregeln zu halten!

Microsoft Office 365: Office-Dokumente aus und in der Cloud

Das neue Microsoft Office ist nicht einfach eine lokale Software, sondern bringt viele Online-Funktionen mit sich. So können vertrauliche Dokumente unbedacht in eine Cloud geraten.

Das Office ist nicht mehr im Büro

Die klassische Bürotätigkeit gibt es zwar noch, doch sie hat viele neue Facetten bekommen. Office-Dokumente werden nicht mehr nur am Schreibtisch im Unternehmen erstellt und bearbeitet, sondern auch unterwegs im Zug, im Hotel, auf der Messe oder daheim im Wohnzimmer. Die Computerarbeit wird immer flexibler. Mobile Endgeräte wie Tablets, aber auch Cloud Computing machen's möglich. So lassen sich Office-Lösungen mittlerweile nutzen, ohne sie auf dem jeweiligen Endgerät zu installieren. Office-Programme laufen dann in der Cloud, Office-Dokumente werden in einer Cloud gespeichert und bearbeitet.

Dokumente sind nicht mehr an Gerät und Ort gebunden

Microsoft Office steht inzwischen geräteübergreifend auf iPhones, iPads, Android-Smartphones, Android-Tablets und durch Windows 10 auch für Windows Phone und Windows Tablet zur Verfügung. Von verschiedenen Geräten aus lässt sich auf die Office-Funktionen und auf die Office-Dokumente zugreifen.

Die große Unabhängigkeit und Flexibilität bedeutet aber auch, dass es nicht mehr so einfach ist, zu sagen, wo sich ein Dokument befindet. Denn es ist irgendwo in der Cloud. Bei Dokumenten, die vertraulich sind und geschützt werden müssen, ist dies kein wirklich gutes Gefühl. Deshalb ist eine wesentliche Forderung der Datenschützer, dass bei Cloud Computing immer klar sein muss, wo sich die Daten genau befinden.

Lokales Office lässt sich mit Cloud kombinieren

Unternehmen und Anwender, die lieber keine Cloud-Lösung einsetzen möchten, wählen dann zum Beispiel Office Professional Plus. Doch je nach Office-Lizenz kann die lokale Software Teil eines Cloud-Vertrags sein, also Bestandteil des Office-365-Abonnements. Dann stehen dem Unternehmen und den Nutzern unter anderem je Anwender 1 TB Datenspeicher mit Freigabeoption sowie Office-Apps auf Tablets und Smartphones zur Verfügung. Das lokale Office hat dann womöglich Außenstellen auf den mobilen Endgeräten sowie einen großen Speicherplatz in der Microsoft-Cloud im Gepäck. In diesem Fall kommt es sehr genau auf die Zugangskontrolle und auf die Dokumentenfreigaben an.

Dokumente müssen vor ungewollter Freigabe geschützt werden

Office 365 als Cloud-Lösung soll nicht nur das flexible, sondern auch das vernetzte Arbeiten unterstützen. Deshalb lassen sich Dokumente auch für andere Nutzer freigeben. Die Einladung zur gemeinsamen Bearbeitung von Dokumenten erfolgt in der Regel durch Weiterleitung eines Dokumenten-Links per E-Mail. E-Mails jedoch können bekanntlich an den falschen Empfänger geschickt oder als unverschlüsselte Nachricht abgefangen und ausspioniert werden. Deshalb sollte unbedingt zusätzlich ein Passwort für den Dokumentenzugriff verlangt und nur genau definierte Nutzer zur Bearbeitung und Einsicht zugelassen werden. Dokumentenfreigaben müssen immer sehr genau geprüft werden.

Ein Office aus der Wolke braucht einen klaren Blick

Eine Office-Lösung aus der Cloud wie Microsoft Office 365 bedeutet, dass Textverarbeitung, Tabellenkalkulation und Präsentationserstellung in der Cloud erfolgen können, die Dokumente damit also dann zu Cloud-Dateien werden können. Ob dies den Sicherheits- und Datenschutzrichtlinien Ihres Unternehmens entspricht, wird vom Schutzbedarf der Daten abhängen.

In jedem Fall sollten Sie so praktisch klingende Funktionen für die Online-Zusammenarbeit nicht unüberlegt einsetzen. Moderne Office-Lösungen aus der Cloud erfordern auch einen Datenschutz für die Cloud - und nicht nur einen Datenschutz am Büroarbeitsplatz.

Überprüfen Sie Ihr Wissen...

Frage: Dokumente werden nur dann in der Cloud gespeichert, wenn ich sie dafür freigebe. Stimmt das?

a) Ja, andernfalls landen die Dokumente auf der Festplatte.
b) Nein, wenn eine Office-Lösung als geräteübergreifend bezeichnet wird, ist das Speichern in der Cloud nicht die Ausnahme, sondern die Regel.

Lösung: Die Antwort b) ist richtig. Jedes Unternehmen und jeder Nutzer sollte prüfen, welchen Standard-Speicherort die Office-Lösungen vorsehen. Oftmals ist das Speichern in der Cloud der Standard. Ändern Sie dies über die Einstellungen, sodass nicht fortlaufend jedes (vertrauliche) Dokument automatisch in der Cloud landet.

Frage: Werden Dokumente über die Cloud an Dritte weitergegeben, können nur diese die Dateien öffnen. Ist das so?

a) Das kommt auf die Sicherheitsmechanismen der Office-Lösung an.
b) Natürlich, denn die Freigabe erfolgt immer für bestimmte Personen.

Lösung: Die Antwort a) ist dieses Mal richtig. Wenn die Freigabe durch Weiterleitung eines Links zum Speicherplatz in der Cloud stattfindet, kann jeder Empfänger des Links das Dokument öffnen. Wird eine unverschlüsselte Mail zur Weitergabe des Links genutzt, könnte die Mail fehlgeleitet oder abgefangen werden. Deshalb sollten Sie zusätzlich zumindest Passwortabfragen vorsehen. Dabei darf das Passwort nicht in der Mail genannt sein.