

# NEWSLETTER DATENSCHUTZ



## Liebe Leserin, lieber Leser,

die DSGVO findet im privaten Bereich keine Anwendung. Doch wo sind die Grenzen zwischen privaten und geschäftlichen Aktivitäten und wie ist mit Mischformen umzugehen?

Kameras zur Kennzeichen-Erfassung auf Parkplätzen bieten viele neue Möglichkeiten: Das Einfahren ohne Zugangskarte und eine automatische Abrechnung erleichtern Nutzern und Anbietern den Alltag. Wie dabei der Datenschutz gewährleistet wird, zeigt unser Beitrag zum Thema.

tet wird, zeigt unser Beitrag zum Thema.

Im Internet lauern immer wieder neue Gefahren und Angreifer finden ständig neue Wege, Sicherheitslücken auszunutzen. Einen starken Schutz für Ihre Nutzerkonten bietet die mittlerweile weit verbreitete Zwei-Faktor-Authentifizierung. Was das ist, wie Angreifer diesen Schutz dennoch durchbrechen konnten und wie Sie sich schützen, erfahren Sie ebenfalls in unserem aktuellen Newsletter.

Wir wünschen Ihnen interessante Erkenntnisse beim Lesen!

**Dr. Uwe Günther**

Beratungsfeldleiter Datenschutz, Curacon GmbH  
Geschäftsführer, Sanovis GmbH

**Stefan Strüwe**

Beratungsfeldleiter Datenschutz, Curacon GmbH

## April\_2021

- 1 PRIVATE AKTIVITÄTEN und die DSGVO
- 2 KENNZEICHEN-KAMERAS beim Parken
- 3 SESSION-COOKIES nicht zu lange speichern

# 1

## PRIVATE AKTIVITÄTEN UND DIE DSGVO

Immer wieder hört man, dass die DSGVO nicht gilt, wenn jemand Daten für private Zwecke verarbeitet. Was ist da dran? Und wo verlaufen die Grenzen?

### Eine Ausnahme vom Anwendungsbereich der DSGVO

Der Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO) geht sehr weit. Aber für die private Verarbeitung von Daten gilt sie tatsächlich nicht. Genauer: Sie gilt nicht für die Verarbeitung personenbezogener Daten „durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.“ So beschreibt es an etwas versteckter Stelle Art. 2 Absatz 2 Buchstabe c DSGVO.

Hinter der Regelung steht der Gedanke, dass rein private Aktivitäten die Interessen anderer Personen normalerweise nicht berühren.

### Ausnahmen sind eng auszulegen

Die DSGVO lässt hier eine Ausnahme von ihrem Anwendungsbereich zu. Ausnahmen sind generell eng auszulegen. Deshalb empfiehlt es sich, die Regelung sehr genau anzuschauen. Dabei ergeben sich wichtige Aspekte:

### Natürliche und juristische Personen

- Die Ausnahme betrifft nur die Verarbeitung von Daten durch „natürliche Personen“. Das sind alle Menschen. Der Gegenbegriff dazu sind „juristische Personen“. Das heißt konkret: Wenn Herr Meier für sich persönlich einen Geburtstagskalender mit seinen Bekannten führt, spielt die DSGVO keine Rolle. Denn dies tut er als natürliche Person. Führt er einen Geburtstagskalender mit

demselben Inhalt dagegen als Geschäftsführer für die Meier GmbH, sieht es anders aus. Dann gilt dafür die DSGVO.

### Persönliche und geschäftliche Tätigkeiten

- Die Ausnahme erfasst nur „persönliche und familiäre Tätigkeiten“. Das Gegenstück dazu sind vor allem „geschäftliche Tätigkeiten“. Ein elektronisches Telefonbuch mit den Rufnummern von Verwandten und persönlichen Freunden interessiert die DSGVO nicht. Bei einem elektronischen Telefonbuch mit den Rufnummern von Geschäftspartnern sieht das anders aus.

### Behandlung von gemischten Fällen

- Dieses Beispiel führt zu „Mischfällen“, die in der Praxis relativ häufig sind. Jemand hat in seinem privaten Handy die Rufnummern von Verwandten und Freunden gespeichert. Außerdem finden sich dort auch die Nummern aller wichtigen Geschäftspartner. Private Verbindungen bestehen zu den Geschäftspartnern nicht. Hier gilt die DSGVO für das gesamte Nummernverzeichnis, also für alle Daten. Denn von der DSGVO ausgenommen sind nur Tätigkeiten, die „ausschließlich“ persönlicher oder familiärer Natur sind. Hier dient das Verzeichnis aber auch geschäftlichen Zwecken.

### Im Zweifel: keine Ausnahme möglich!

Unsicherheiten bei der Abgrenzung gehen immer zulasten dessen, der die Daten verarbeitet. Im Zweifel gilt die DSGVO also, und eine Berufung auf die Ausnahme ist nicht möglich. Beispiel: Es bleibt unklar, ob jemand einen Geburtstagskalender als Privatmann oder als Geschäftsführer nutzt. Dann muss er die DSGVO



voll beachten. Er kann sich nicht auf die Ausnahme von der DSGVO berufen.

#### **Soziale Netzwerke ohne Zugriffsbeschränkung**

Viele wollen ihre Fotos einem weiteren Kreis von Bekannten zugänglich machen und stellen sie beispielsweise bei Facebook ein. Ansehen kann sie jeder, der auf den Account zugreift. Damit befinden sich die Aufnahmen außerhalb des ausschließlich privaten Bereichs. In solchen Fällen gilt die DSGVO in vollem Umfang.

#### **Echt private Gruppen in sozialen Netzwerken**

Natürlich sind auch in sozialen Netzwerken rein private Gruppen möglich. Beispiel: Weit voneinander entfernt lebende Mitglieder einer Familie richten eine private Gruppe ein, in der sie private Bilder und private Nachrichten austauschen. Zugriff haben nur die Mitglieder. Dafür gilt die DSGVO nicht. Wichtig ist aber eine persönliche Verbundenheit der Gruppe untereinander.

#### **„Zahlenspiele“ helfen nicht weiter**

Keine Rolle spielt dagegen, wie viele Mitglieder zu einer Gruppe gehören. Bloß weil eine

Gruppe beispielsweise nur fünf oder zehn Mitglieder hat, ist sie nicht automatisch eine private Gruppe. Umgekehrt können beispielsweise bei einer großen Familie auch 20 oder 30 Personen durchaus noch eine private Gruppe bilden.

#### **Überwachungskamera in der eigenen Wohnung**

Manche lassen in ihrer Wohnung eine Kamera laufen, wenn sie außer Haus sind. Das tut etwa ein Katzenfreund, der tagsüber immer wieder einmal aus der Entfernung sehen will, wie es der Kätzin mit den neu geborenen Kätzchen geht. Das ist eindeutig ein Fall rein privater Datenverarbeitung, auch wenn der Zugriff über eine Datenleitung aus der Ferne erfolgt.

#### **Überwachungskamera vor dem eigenen Haus**

Anders sieht es bei Kameras in Hauseinfahrten aus. Das akzeptieren die Datenschutzbehörden nicht mehr als private Datenverarbeitung. Der Grund: Eine solche Überwachung dient dazu, Störenfriede im Bild festzuhalten. Das geht dann schon über den internen, rein privaten Bereich hinaus.

---

## **2 KENNZEICHEN-KAMERAS BEIM PARKEN**

**An immer mehr Parkplätzen verschwinden die Einfahrtsschranken. Stattdessen erfassen Kameras die Kennzeichen. Wie ist das mit dem Datenschutz zu vereinbaren?**

#### **Einfahrtsschranke – das ist Vergangenheit!**

Immer mehr Unternehmen bauen an der Einfahrt zum Firmenparkplatz die Einfahrtsschranke ab. Stattdessen filmen sie die Kennzeichen der einfahrenden Fahrzeuge. In einer Datenbank lässt sich feststellen, ob dieses Fahrzeug den Parkplatz benutzen darf.

Ähnlich verfahren die Betreiber von öffentlichen Parkhäusern. Hineinfahren kann jeder einfach so. Bezahlt wird am Automaten, nachdem der Fahrer sein Kennzeichen eingegeben hat.

#### **Mehr Bequemlichkeit beim Parken**

Die Vorteile liegen auf der Hand. Kein Fahrer muss mehr die Scheibe an der Fahrtür öffnen, nach dem Einfahrtschip kramen oder mühsam das Parkticket bei der Einfahrt lösen. Bei der Bezahlung muss man kein Einfahrtticket mehr in den Automaten stecken. Stattdessen gibt man sein Kennzeichen ein.

#### **Kfz-Kennzeichen sind personenbezogen**

Der Datenschutz ist ein Thema, weil die Kennzeichen von Fahrzeugen personenbezogene Daten enthalten. Das überrascht auf den ersten

Blick. Aber: Mithilfe des Kennzeichens ist es leicht möglich, den Halter eines Fahrzeugs festzustellen. Genau dazu sind sie da. Wer Kennzeichen festhält, muss deshalb die Datenschutzregelungen beachten.

### **Kaum Probleme bei Firmenparkplätzen**

Bei einem Firmenparkplatz ist alles relativ einfach. Seine Benutzung ist in irgendeiner Weise im Zusammenhang mit dem Arbeitsverhältnis geregelt. Beispielsweise kann der Arbeitsvertrag eine entsprechende Klausel enthalten. Vielleicht gibt es auch eine Betriebsvereinbarung. Arbeitsvertrag oder Betriebsvereinbarung sind dann die Rechtsgrundlage dafür, dass der Arbeitgeber die nötigen Daten festhalten darf.

Meist kosten Firmenparkplätze nichts. Dann genügt es, die Parkberechtigung festzustellen. Dazu sind die Kennzeichen der berechtigten Fahrzeuge in einer Datenbank gespeichert. Fährt ein Fahrzeug in den Parkplatz ein, wird sein Kennzeichen mit dieser Datenbank abgeglichen.

### **Daten für die Abrechnung**

Kostet ein Parkplatz etwas, braucht man zusätzlich Daten für die Abrechnung. Bei öffentlichen Parkplätzen ist das die Regel. Abgerechnet wird bei der Ausfahrt. Dazu braucht man Einfahrtszeit und Ausfahrtszeit. Manchmal bestehen Monatsverträge für Dauerparker. Bei ihnen spielen die Parkzeiten normalerweise keine Rolle. Dann sind diese Daten auch nicht nötig.

### **Datenschutzhinweise bei der Einfahrt**

Ein häufiges Konfliktthema sind die Datenschutzhinweise an der Einfahrt zum Parkplatz. Bei einem Firmenparkplatz für Beschäftigte können sie entweder sehr kurz ausfallen oder sogar völlig wegbleiben. Die Beschäftigten sind im Regelfall auch ohne solche Hinweise ausreichend informiert. So steht beispielsweise in Betriebsvereinbarungen für Firmenparkplätze meist auch, welche Daten gespeichert werden dürfen und was mit ihnen geschieht.

### **Parkhäuser mit engen Einfahrten**

Bei Parkhäusern ist es nicht ganz so einfach. Typisch ist folgende Situation: Wer parken will, merkt erst an der Einfahrt, dass es keine Schranke gibt. Oft genug sind die Einfahrten eng. Für große Schilder mit ausführlichen Informationen ist schlicht kein Platz. Die Datenschutz-Grundverordnung verlangt aber, dass eine umfassende Information über die Verarbeitung der Daten erfolgt.

### **Vernünftige Lösungen für die Praxis**

Für solche Fälle sind die Datenschutzbehörden mit praxisnahen Lösungen einverstanden. Sie sehen so aus: An der Einfahrt steht ein Schild, das auf die Kennzeichenerfassung hinweist. Ansonsten heißt es dort lediglich: „Weitere Informationen im Parkhaus. Freie Ausfahrt binnen 10 Minuten möglich.“ Diese Formulierung ist nur ein Beispiel, es sind auch andere kurze Texte möglich.

### **Wem es nicht gefällt, kann kostenlos ausfahren**

Wer einfährt, kann sich dann im Parkhaus informieren, wie die Kennzeichenerfassung erfolgt und welche Daten gespeichert werden. Ist er damit nicht einverstanden, kann er sich wieder ins Auto setzen und gebührenfrei ausfahren. Sein Kennzeichen wurde dann zwar bei der Einfahrt erfasst. Das System ist aber so eingestellt, dass es diese Daten vollständig löscht, wenn das Fahrzeug innerhalb der Karenzzeit ausfährt.

### **Bequemlichkeit und Datenschutz – das geht!**

Insgesamt ist die Kennzeichenerfassung auf Parkplätzen ein Beispiel dafür, dass Bequemlichkeit

und Datenschutz wunderbar zusammenpassen können. Es ist deshalb kein Wunder, dass immer mehr Supermärkte und Einkaufszentren solche Systeme einsetzen.



# 3

## SESSION-COOKIES

### NICHT ZU LANGE SPEICHERN

**Sicherheitsbehörden warnen aktuell davor, dass Angreifer selbst Online-Sitzungen, die über Zwei-Faktor-Authentifizierung geschützt werden, mittels Cookie-Diebstahl übernehmen könnten. Achten Sie deshalb auf das richtige Vorgehen mit dem Webbrowser.**

#### Erhöhter Schutz für den Zugang zu Daten

Online-Shops müssen die Anforderungen der zweiten EU-Zahlungsdiensterichtlinie PSD2 an die starke Kundenauthentifizierung (Strong Customer Authentication – SCA) erfüllen: Kunden müssen bei Transaktionen im Web und in Apps ihre Identität über mindestens zwei von drei möglichen, voneinander unabhängigen Sicherheitsfaktoren belegen. Neben einem Passwort (Sicherheitsfaktor Wissen) wird so zusätzlich beispielsweise der Fingerabdruck (Biometrie) erforderlich.

Diese sogenannte Zwei-Faktor-Authentifizierung (kurz 2FA) ist auch aus dem Online-Banking bekannt. Damit lässt sich ein erhöhter Zugangsschutz realisieren. Selbst dann, wenn ein Angreifer das Passwort eines Nutzers erbeutet, kann er sich nicht anmelden. Es fehlt dann zum Beispiel der Fingerabdruck des Nutzers, um seine Identität zu bestätigen.

#### Session-Cookie identifiziert einen angemeldeten Nutzer

Die Speicherung dieser Session-Cookies (oder Sitzungs-Cookies) ist erforderlich, damit man sich nicht auf jeder neuen Seite neu anmelden muss. Laut einer Meldung der US-amerikanischen Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) gelang es Angreifern, diese Funktion auszunutzen und so Zugriff auf Konten zu erlangen, obwohl diese mit einer Zwei-Faktor-Authentifizierung geschützt waren. Hierzu mussten die Angreifer den gespeicherten Session-Cookie stehlen um die laufende Sitzung zu übernehmen.

#### Es kommt auf das richtige Nutzerverhalten an

Um Ihre Online-Zugänge besser zu schützen achten Sie darauf, dass die Sitzungs-Cookies so kurz wie möglich gespeichert werden. Melden Sie sich ab und schließen Sie den Browser vollständig, wenn Sie einen Zugang aktuell nicht mehr benötigen.

Ist der Browser geschlossen, wird der Session-Cookie ungültig.

## Schützen Sie Ihre Online-Zugänge richtig? Machen Sie den Test!



**Wenn mein Passwort um einen Fingerabdruck bei der Anmeldung ergänzt wird, kann keiner meinen Online-Zugang zum Webshop oder zum Online-Banking übernehmen. Stimmt das?**

1. Nein, selbst eine Zwei-Faktor-Authentifizierung im Browser lässt sich umgehen, zum Beispiel durch Entführung des Session-Cookies.
2. Ja, denn wer sollte meinen Fingerabdruck fälschen können?

### Lösung:

Die Antwort 1. ist richtig. Leider können Angreifer Sitzungscookies stehlen und missbrauchen, um damit bestehende Online-Sitzungen zu übernehmen. Der Diebstahl des Cookies ist dabei ein Diebstahl der digitalen Identität. Beenden Sie deshalb nach der Abmeldung von einem Online-Dienst immer auch den Browser.



**Blockiere ich alle Cookies über den Browser, erhöht dies den Zugangsschutz. Stimmt das?**

1. Ja, denn ohne Cookies im Browser können auch keine Cookies gestohlen werden. So kann ich das Aushebeln des Zugangsschutzes vermeiden.
2. Nein, denn der Browser braucht die Sitzungscookies, um wie gewünscht zu funktionieren. Sogenannte technische Cookies (zum Beispiel für die Warenkorb-Funktion) sollte man nicht blockieren.

### Lösung:

Die Antwort 2. ist richtig. Eine vollständige Blockade von Cookies kann zwar die feindliche Übernahme von Sitzungscookies und laufenden Online-Sitzungen verhindern. Aber dann arbeiten Webbrowser, Online-Shop und Online-Bank nicht mehr wie gewünscht und erforderlich.

Sitzungscookies verhindern, dass Sie sich als Nutzer fortlaufend im Online-Shop anmelden müssen während eines Shopping-Vorgangs. Ohne Cookies können Sie keine Produkte im Online-Warenkorb sammeln und gemeinsam bezahlen. Deshalb müssen Sie die Session Cookies durch den richtigen Umgang mit dem Webbrowser besser schützen. Es hilft nicht, einfach alle Cookies zu blockieren.

#### IMPRESSUM

##### Redaktion

**Dr. Uwe Günther**

**Sanovis GmbH**

Riedenburger Straße 7

81677 München

089 9927579-22

Uwe.Guenther@Sanovis.com

**Stefan Strüwe, RA**

**CURACON GmbH Wirtschaftsprüfungsgesellschaft**

Am Mittelhafen 14

48155 Münster

0251 92208-209

Stefan.Struewe@Curacon.de