

Sehr geehrte Damen und Herren,  
liebe Kundinnen und Kunden,

die rechtskonforme Ausgestaltung der Cookie-Banner auf Webseiten ist ein wiederkehrendes Thema in unseren mip Beratungsinformationen sowie in persönlichen Gesprächen mit unseren Kund:innen im Rahmen der Überprüfung ihrer Webseiten. Nunmehr haben Maximilian Schrems und auch die Berliner Datenschutzaufsicht jeweils die Cookie-Banner von diversen Webseiten geprüft und Mängel festgestellt.



Ferner haben wir in der Ausgabe einen Hinweis auf eine Entscheidung der Aufsichtsbehörde Niedersachsen aufgenommen, die sich mit den Fragen des technischen Datenschutzes bei einem Web-Shop befasst hat. Der Betreiber soll nun ein Bußgeld in Höhe von 65.500 EUR zahlen.

Sie finden außerdem noch zwei Gerichtsentscheidungen zu den Themen „Datenübermittlung an Auskunfteien“ und „Videoüberwachung“ in dieser Ausgabe.

Für unsere Kunden aus dem Automotivsegment haben wir am Schluss noch eine Info zu einer Leitlinie, die der Europäische Datenschutzausschuss (EDSA) zum Datenschutz bei vernetzten Fahrzeugen herausgegeben hat.

Sie sehen, beim Thema Datenschutz ist viel in Bewegung und es bedarf einer regelmäßigen Prüfung und Umsetzung. Wir behalten die relevanten Themen für Sie im Blick und unterstützen Sie bei den anstehenden Themen.

Ihr

Asmus Eggert

---

## Inhalt

Schrems reicht 422 formelle DSGVO-Beschwerden gegen Cookie-Banner ein .....	2
Berliner Datenschutzbeauftragte schreibt 50 Webseiten-Betreiber wegen rechtwidrigem Tracking an .....	2
Aufsichtsbehörde Niedersachsen verhängt 65.500 EUR DSGVO-Bußgeld gegen Online-Shop wegen veralteter Technik.....	3
OLG Naumburg: Datenübermittlung an Auskunftei.....	3
OVG Koblenz: Ausgeschaltete Videokamera unterfällt nicht der DSGVO.....	4
Leitlinien zur Verarbeitung personenbezogener Daten bei vernetzten Fahrzeugen .....	5

---

**Hinweis:** Als externe Datenschutzbeauftragte sind wir nach Art. 39 Abs. 1 a) DSGVO verpflichtet, unsere Kund:innen über ihre datenschutzrechtlichen Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der EU bzw. der Mitgliedstaaten zu beraten und zu unterrichten. Mit der mip Beratungsinformation unterrichten wir unsere Datenschutzkund:innen im Rahmen dieser Pflicht über aktuelle Entwicklungen in der Gesetzgebung, Rechtsprechung und Literatur sowie über Maßnahmen der Aufsichtsbehörden.

## Schrems reicht 422 formelle DSGVO-Beschwerden gegen Cookie-Banner ein

Der Verein des Datenschutzaktivisten Maximilian Schems, noyb, hat am 10.08.2021 422 formale Beschwerden bei zehn Datenschutzbehörden eingereicht. Dem ist der Versand von Warnungen und "Beschwerdeentwürfen" Ende Mai dieses Jahres an mehr als 500 Unternehmen vorausgegangen. Laut der Presseerklärung des Vereins hatten die Unternehmen 42 % aller Verstöße behoben. 82 % aller Unternehmen hätten allerdings ihr DSGVO-widriges Handeln nicht vollständig eingestellt.

Ein rechtskonformes Cookie-Banner, das Einwilligungen zum Setzen von Cookies einholt, erfordert, dass der Widerruf der Einwilligung so einfach ausgestaltet sein muss, wie deren Abgabe. Laut Schrems erfüllen nur 18 % der geprüften Seiten diese Anforderung, in dem sie ein sichtbares "Widerrufssymbol" anzeigen. Er stellt bei den Unternehmen gerade in diesem Punkt nur geringe Anpassungsbereitschaft bzw. großes Beharrungsvermögen fest.

Die Umsetzung des Datenschutzes und das Interesse des Webseitenbetreibers an der Auswertung des Nutzerverhaltens stellt ein schwieriges Spannungsfeld dar. Damit ist die Ausgestaltung eines Cookie-Banners eine Risikoentscheidung des Webseitenbetreibers. Mit dieser Aktion hat noyb eine Vielzahl von Verfahren angestoßen, die in aufsichtsbehördliche Entscheidungen und ggf. in eine gerichtliche Überprüfung münden werden. Damit realisiert sich das Risiko eines Bußgeldes für die überprüften Unternehmen.

## Berliner Datenschutzbeauftragte schreibt 50 Webseiten-Betreiber wegen rechtswidrigem Tracking an

Am 09.08.2021 hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit darüber informiert, dass sie in einer Aktion rund 50 Berliner Unternehmen schriftlich aufgefordert habe, das Tracking auf ihren Webseiten in Einklang mit den geltenden Datenschutzregeln zu bringen. Andernfalls werde die Aufsichtsbehörde förmliche Prüfverfahren einleiten, die zu einer Anordnung oder einem Bußgeld führen können. Damit schlägt sie in die gleiche Kerbe wie noyb.

„Die Rechtslage ist eindeutig: Wenn Webseiten-Betreibende das Verhalten ihrer Nutzer:innen mit Hilfe von Cookies und anderen Technologien verfolgen wollen, benötigen sie dafür eine Rechtsgrundlage“, sagt Maja Smoltczyk, Berliner Beauftragte für Datenschutz und Informationsfreiheit. Auch wenn viele Webseiten mittlerweile differenzierte Cookie-Banner mit mehreren Ebenen anzeigen, werde hiermit häufig gar keine wirksame Einwilligung eingeholt.

Auch die Berliner Behörde macht deutlich, dass es eine Grundvoraussetzung ist, dass es ebenso einfach sein muss, das Tracking abzulehnen, wie darin einzuwilligen. „Die Ablehnung darf nicht aufwendiger oder gar versteckt sein“, erklärt die Datenschutzbeauftragte. „Zudem werden die Einwilligungsabfragen gerne eingebettet in unvollständige oder missverständliche Angaben und Beschriftungen. Wie die Webseitenbetreibenden bei solch einer Gestaltung nachweisen wollen, dass die Nutzer:innen freiwillig und informiert zugestimmt haben, ist mir ein Rätsel.“

**Praxishinweis:** Die Berliner Aufsichtsbehörde begründet die Aktion mit einer Vielzahl von Beschwerden, die hierzu bei ihr eingegangen seien. Das zeigt aus unserer Sicht, dass die Nutzer für die Gestaltung der Banner sensibler werden. Webseiten-Betreiber sollten die Ankündigung daher zum Anlass nehmen, die Cookie-Banner auf ihren Webseiten zu prüfen und ggfs. anzupassen.

Laut Pressemeldung hat die Behörde die Verantwortlichen aufgefordert, die Datenverarbeitung unverzüglich in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen. Es erfolge in jedem Fall eine zweite Prüfung der Webseiten. Je nachdem, ob vergangene und/oder andauernde Verstöße festgestellt würden, könne das weitere Maßnahmen der Behörde nach sich ziehen.

## Aufsichtsbehörde Niedersachsen verhängt 65.500 EUR DSGVO-Bußgeld gegen Online-Shop wegen veralteter Technik

Die Datenschutzbeauftragte Niedersachsens hat in ihrem [Tätigkeitsbericht 2020](#) mitgeteilt, dass sie gegen einen Online-Shop wegen veralteter Technik ein DSGVO-Bußgeld i. H. v. 65.500 EUR verhängt habe.

Anlass war die unzureichende Umsetzung der technisch-organisatorischen Maßnahmen (TOM) auf der besagten Webseite. Zum einen hatte der Shopanbieter eine Webshop-Anwendung genutzt, die seit 2014 veraltet war und vom Software-Hersteller seitdem nicht mehr mit Sicherheitsupdates versorgt wurde. Außerdem stellte die Aufsichtsbehörde fest, dass die in der Datenbank abgelegten Passwörter zwar mit der kryptographischen Hashfunktion „MD5“ gesichert waren, die allerdings nicht auf den Einsatz für Passwörter ausgelegt gewesen sei. Eine schnelle Berechnung der Klartext-Passwörter sei daher möglich gewesen. Auch existierten sog. „Rainbow-Tables“ im Internet, anhand derer - ganz ohne Berechnung - das zu einem Hash gehörige Passwort abgelesen hätte werden können. Hinzu sei gekommen, dass kein „Salt“ verwendet wurde. Ein solcher Salt, der für jedes Passwort individuell generiert wird, verlängert ein Passwort und erschwert so die systematische Berechnung deutlich. Ziel des Salt ist es, dass der Angreifer für jedes Passwort eine komplette Neuberechnung durchführen muss und vorgefertigte Rainbow-Tables wertlos werden. Ohne Salt genügte hingegen eine gemeinsame Berechnung für die komplette heruntergeladene Datenbank.

Die Aufsichtsbehörde kam daher zum Schluss, dass die TOM keinen ausreichenden Schutz der personenbezogenen Daten darstellen. Ein Angreifer hätte die Passwörter leicht ermitteln und damit z.B. bei den ebenfalls in der Datenbank hinterlegten E-Mail-Adressen testen und im Erfolgsfall erhebliche (Folge-)Schäden anrichten können.

Bei der Bestimmung der Sanktionshöhe habe man allerdings strafmildernd berücksichtigt, dass der betroffene Shop bereits vor dem Bußgeldverfahren seine Kunden darüber informiert hatte, dass ein Wechsel des Passwortes notwendig sei.

**Praxishinweis:** Das aktuelle Beispiel zeigt, dass TOM einer regelmäßigen Prüfung unterzogen werden müssen. Unternehmen müssen beim Einsatz von Hard- und Software sicherstellen, dass die vom Hersteller bereitgestellten Sicherheitsupdates eingespielt werden. Dazu ist z.B. zu regeln, wer hierfür verantwortlich ist (idealerweise zentrale Verwaltung über die IT). Außerdem muss regelmäßig geprüft werden, ob der Verpflichtung auch zeitnah nachgekommen worden ist.

Daneben gilt es, etwaige rechtliche Veränderungen zu berücksichtigen. Aber auch die technischen Maßnahmen sind regelmäßig mit dem aktuellen Stand der Technik abzugleichen. Was gestern noch erlaubt und sicher war, muss es heute längst nicht mehr sein. Dies gilt insbesondere für Verschlüsselungstechnologien.

## OLG Naumburg: Datenübermittlung an Auskunftfei

Anfang des Jahres hat sich das OLG Naumburg im Urteil vom 10.03.2021 – 5 U 182/20 (LG Halle) mit der Rechtmäßigkeit der Weiterleitung von Daten an eine Auskunftfei befasst. Danach stelle die Weiterleitung von Daten, die zum Zwecke des Forderungsmanagements an ein Inkassounternehmen und eine Auskunftfei übermittelt werden, die zuvor durch den Auftraggeber zum Zwecke der Vertragserfüllung erhoben wurden, jedenfalls eine kompatible Zweckänderung i.S.v. Art. 6 Abs. 4 DSGVO dar. Die Datenübermittlung ist danach zulässig nach Art. 6 Abs. 1 lit. b) 1. Alt. DSGVO.

Eine derartige Datenübermittlung könne sich laut Gericht auch auf Art. 6 Abs. 1 lit. f) DSGVO, also das berechtigte Interesse, stützen. Die Datenübermittlungen dienen dazu, durch Zurverfügungstellung von bonitätsrelevanten Daten über den Betroffenen andere

Vertragsunternehmen der Auskunftspflicht vor wirtschaftlichen Schäden zu schützen. Ein berechtigtes Interesse bestehe jedoch nur hinsichtlich solcher Forderungen, die die Voraussetzungen des § 31 Abs. 2 BDSG erfüllen. Das ist z. B. insbesondere bei Forderungen der Fall, bei denen

- a) *der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,*
- b) *die erste Mahnung mindestens vier Wochen zurückliegt,*
- c) *der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftspflicht unterrichtet worden ist und*
- d) *der Schuldner die Forderung nicht bestritten hat.*

**Praxishinweis:** Wenn Ihr Unternehmen Daten an Auskunftsebenen weiterleitet, nehmen Sie den Hinweis zum Anlass, das Verzeichnis der Verarbeitungstätigkeiten auf dieses Verfahren zu prüfen, insbesondere ob die Voraussetzungen des § 31 Abs. 2 BDSG eingehalten werden. Klären Sie ab, ob Sie auf die richtige Rechtsgrundlage abstellen und entsprechend in der Datenschutzerklärung über diese Verarbeitung aufklären.

## OVG Koblenz: Ausgeschaltete Videokamera unterfällt nicht der DSGVO

Die Videoüberwachung von öffentlichen und nicht öffentlichen Räumen ist regelmäßig Gegenstand datenschutzrechtlicher Überprüfungen. Das OVG Koblenz hatte nun einen Fall zu entscheiden ([Urt. v. 25.06.2021, Az: 10 A 10302/21](#)), bei dem es um die Rechtmäßigkeit einer datenschutzrechtlichen Anordnung des Abbaus einer Videokamera durch eine Aufsichtsbehörde ging, die vom Eigentümer nicht mehr betrieben wurde. Die deaktivierte Kamera war an einem Mast auf dem Parkplatz eines Einkaufszentrums angebracht.

Das Gericht hat klargestellt, dass eine ausgeschaltete Kamera keine personenbezogenen Daten verarbeitet und damit der sachliche Anwendungsbereich der DSGVO im Hinblick auf die bloß vorhandene, aber deaktivierte Kamera nicht eröffnet sei.

Die Aufsichtsbehörde sei damit auch nicht berechtigt, mit der angefochtenen Anordnung die Demontage der Kamera zu verlangen. Nach Art. 58 Abs. 2 lit. f) DSGVO verfüge die Aufsichtsbehörde im Fall eines Datenschutzverstößes über sämtliche Abhilfebefugnisse, die es ihr (...) gestatten, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. (...) Eine weitergehende Befugnis zur Anordnung auch des Abbaus der Kamera begründet Art. 58 Abs. 2 lit. f) DSGVO nicht. Vielmehr ermächtigt die Norm die Aufsichtsbehörde ihrem eindeutigen Wortlaut nach allein dazu, die Verarbeitung vorübergehend oder ganz zu beschränken bzw. zu verbieten.

**Praxishinweis:** Alle Menschen haben das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass ihr Verhalten permanent mit einer Kamera beobachtet oder aufgezeichnet wird. Im Alltag ist Videoüberwachung dennoch weit verbreitet, weil die Technologie sehr preisgünstig geworden ist. Eine dauerhafte und anlasslose Videoüberwachung in der Öffentlichkeit greift allerdings erheblich in die Grundrechte von Personen ein. Daraus folgt, dass Betreiber:innen einer Videoanlage verpflichtet sind, eine Reihe gesetzlicher Voraussetzungen zu beachten. Ist in einem Unternehmen die Einführung einer Videoüberwachung geplant, ist die/der Datenschutzbeauftragte einzubeziehen. Die Zwecke sind sauber zu definieren und festzulegen, die Verarbeitungstätigkeit ist in das Verzeichnis der Verarbeitungstätigkeiten aufzunehmen, es ist eine Datenschutzfolgeabschätzung durchzuführen, TOM sind zu ergreifen, es muss informiert werden (Hinweisschilder) etc. Die Datenschutzkonferenz (DSK) hat einen [Leitfaden](#) zu dem Thema veröffentlicht, der eine gute Übersicht gibt.

Hier positioniert sich die DSK auch zur viel diskutierten Frage des Einsatzes von Kameraattrappen: Wie auch das OVG wird hier kein Anwendungsfall der DSGVO gesehen. Allerdings könne durch die Attrappe unter Umständen ein so hoher Überwachungsdruck erzeugt werden, der eine Verletzung

der Persönlichkeitsrechte darstelle. Wer eine Attrappe zur Verhaltenssteuerung Dritter einsetzt, müsse damit rechnen, dass zwar nicht datenschutzrechtliche aber zivilrechtliche Abwehransprüche (bspw. auf Unterlassen oder Schadensersatz) gegen ihn oder sie geltend gemacht werden.

## Leitlinien zur Verarbeitung personenbezogener Daten bei vernetzten Fahrzeugen

Der Europäische Datenschutzausschuss (EDSA) hat im März dieses Jahres Leitlinien zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen verabschiedet.

**Praxishinweis:** Die Leitlinien des EDSA sind mehr als nur unverbindliche Empfehlungen. Auch wenn Leitlinien nicht rechtsverbindlich sind, bündeln sie die Auffassung der im EDSA vereinten nationalen Datenschutzaufsichtsbehörden. Folglich muss man davon ausgehen, dass sich die nationalen Aufsichtsbehörden im Rahmen ihrer Aufsichtstätigkeit an diese halten werden. Hinzu kommt, dass der EDSA in seinem jährlichen Bericht die Umsetzung der von ihm erstellten Leitlinien in der Praxis überprüft. Der EDSA übermittelt seinen Jahresbericht dem Europäischen Parlament, dem Rat und der Kommission. Diese können die Feststellungen des EDSA zum Anlass nehmen, eigene Maßnahmen zum Abstellen von Defiziten einzuleiten.

Unternehmen, die im Bereich „vernetzte Fahrzeuge“ oder sonstigen Mobilitätsanwendungen tätig sind, sollten die Leitlinien prüfen und beachten.

### Impressum

#### **mip Consult GmbH**

Wilhelm-Kabus-Straße 9  
10829 Berlin

Tel: +49 (0) 30 – 20 88 999 – 00

Fax: +49 (0) 30 – 20 88 999 – 88

Redaktion: Stefan Ax, Asmus Eggert

Internet: [www.sofortdatenschutz.de](http://www.sofortdatenschutz.de) und [www.blog.sofortdatenschutz.de](http://www.blog.sofortdatenschutz.de)

E-Mail: [sofortdatenschutz@mip-consult.de](mailto:sofortdatenschutz@mip-consult.de)

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider

Registergericht: Amtsgericht Berlin-Charlottenburg

Registernummer: HRB 121869

USt.-Identnr.: DE249276018

Verantwortlich nach § 18 Abs. 2 MStV: Asmus Eggert