

I DIE ZEHN GEBOTE DES DATENSCHUTZES

VERHALTENSCHINWEISE FÜR PRIVATPERSONEN BEI DER NUTZUNG ELEKTRONISCHER KOMMUNIKATIONSMITTEL

Das Internet und die vielfältigen Möglichkeiten der elektronischen Kommunikation bieten viele Vorteile und erleichtern das tägliche Leben ganz erheblich. Außerdem hat die Corona-Pandemie der Digitalisierung einen zusätzlichen Schub nach vorne gegeben. Eigentlich können wir uns heute nicht mehr vorstellen, ohne diese technischen Möglichkeiten auszukommen.

Doch wo Licht ist, ist auch Schatten: So wie es im Straßenverkehr Verkehrsregeln gibt, gibt es auch bei der Nutzung elektronischer Medien Regeln, die beachtet werden sollten. Dazu zählen insbesondere die Regeln des Datenschutzes und des Urheberrechts. Leider sind diese Grundregeln bei vielen Nutzerinnen und Nutzern noch nicht angekommen – es gibt ja auch keinen „elektronischen Führerschein“...

Die folgenden „Zehn Gebote der Nutzung der elektronischen Kommunikation“ sollen daher alle Nutzerinnen und Nutzer unterstützen, sich künftig möglichst unfallfrei durch die unendlichen Weiten des Datenverkehrs zu bewegen:

1. GEBOT

Egal wo – Geben Sie nicht zu viele Informationen über sich selbst preis!

Achten Sie darauf, in Chats, Internetforen, im E-Mail-Austausch mit Fremden, in Messenger-Diensten (z.B. WhatsApp) und in sozialen Netzwerken (z.B. Facebook) außer dem Namen möglichst keine persönlichen Informationen (wie Adresse, Handy- oder Telefonnummer) preiszugeben.

Kostenlose Dienste wie „Facebook“, „Twitter“ benutzen zahllose Daten wie Bilder und Kommentare der Nutzer, sammeln diese und geben diese für Werbezwecke an Dritte weiter. Wichtig ist, die Einstellungen zur Privatsphäre genau zu prüfen und möglichst strikt zu halten. Dies gilt vor allem für Einstellungen wie die Auffindbarkeit des Profils, die Möglichkeit, von Fremden kontaktiert zu werden und das Ausmaß der Sichtbarkeit von Daten innerhalb der Community. Wenn man ein Netzwerk

nicht mehr nutzen möchte, sollte man seine Mitgliedschaft beenden und die Profildaten löschen.

Noch ein Hinweis: Passen Sie immer auf, was Sie posten: Wenn Sie irgendwo im Urlaub in der Südsee sind und unbedingt die ganze Welt über Facebook & Co. an Ihrem Glück teilhaben lassen wollen – lassen Sie das bitte bleiben! Sie teilen nämlich gleichzeitig der ganzen Welt mit, dass Sie gerade nicht zu Hause sind und sich offensichtlich einen teuren Urlaub leisten können. Es ist für alle Menschen mit Internet-Anschluss ein Leichtes, innerhalb weniger Minuten Ihre Wohnanschrift festzustellen und Sie sollten sich nicht wundern, wenn Sie nach Ihrer Rückkehr Ihr Haus leer vorfinden.

2. GEBOT

Thema Urheberrechte und Persönlichkeitsrechte – Seien Sie vorsichtig mit Fotos und fremden Texten!

Klauen Sie niemals fremde Fotos oder Texte aus dem Internet zur Verwendung für eigene Zwecke und senden Sie niemals fremden Personen eigene Fotos und Videos oder Fotos und Videos, die Sie von anderen Personen bekommen haben!

Grundsätzlich gilt: Wer ein Foto anfertigt, der hat auch die Bildrechte. Verwendet man fremde Fotos ohne Einwilligung für eigene Zwecke (z.B. weil man es im Internet gefunden hat, schön findet und es gut auf die eigene Homepage passt) sollte sich nicht wundern, wenn er vom Urheber auf Unterlassung und Schadensersatz verklagt wird. Das geht schneller als man denkt! Dasselbe gilt für Fotos, die man von anderen Personen bekommen hat: Bekommt man Fotos, die andere angefertigt haben, hat man zwar das Recht, diese anzuschauen und ggf. privat zu speichern, aber noch lange nicht, diese ohne Einwilligung des Urhebers auch weiterzuverbreiten!

Bitte seien Sie auch äußerst vorsichtig, wenn Sie eigene Fotos ins Internet stellen, in sozialen Medien posten oder per Mail an Dritte versenden. Sie könnten Persönlichkeitsrechte verletzen!

Grundregel: Stellen Sie – wenn überhaupt – nur ausgewählte eigene Fotos ins Netz. Sollten ande-

DIE ZEHN GEBOTE DES DATENSCHUTZES

re Personen mit darauf zu sehen sein müssen Sie deren Einwilligung einholen. Eine Ausnahme gilt nur für den (engen) privaten/familiären Bereich - seien Sie aber auch hier bitte restriktiv!

Warum das? Ganz einfach: Jeder hat ein (Persönlichkeits-)Recht am eigenen Bild. Das bedeutet, dass ein Foto ohne Einwilligung des Abgebildeten nicht veröffentlicht werden darf. Nirgends und schon gar nicht im Internet! Gerade dort kommt es aber besonders häufig zu Rechtsverstößen. Egal ob Partyfotos oder Urlaubsbilder: Alles Mögliche wird z.B. bei Facebook eingestellt oder über WhatsApp verbreitet – mit teilweise ungeahnten Folgen. So sichert sich z.B. Facebook durch seine Nutzungsbedingungen (denen man arglos zugestimmt hat, um den Dienst überhaupt nutzen zu können) sehr umfangreiche Rechte an allen hochgeladenen Bildern – Pech für Sie, wenn Sie auf diese Weise Urheberrechte und Persönlichkeitsrechte, die sie gar nicht haben, automatisch an Facebook & Co. abgetreten haben!

3. GEBOT

Kinderfotos – bitte lassen Sie das!

Bitte stellen Sie keine Kinderfotos für alle sichtbar in soziale Medien (z.B. Facebook) ein, auf denen Kinder klar zu erkennen sind, verbreiten Sie möglichst keine solche Kinderfotos über Messenger-Dienste (z.B. WhatsApp) und versenden Sie möglichst auch bitte keine Kinderfotos per E-Mail!

Das kennen wir alle: Stolze Eltern und Großeltern verbreiten eifrig Fotos ihrer Kinder und Enkel, um andere Menschen an deren Entwicklungsfortschritten teilhaben zu lassen – über soziale Medien, Messenger-Dienste oder andere elektronische Kommunikationsmittel. In der Urlaubszeit sind beispielsweise Strandfotos äußerst beliebt, auf denen klar identifizierbare Kinder – wenn überhaupt - eher spärlich bekleidet sind. Solche Fotos gehören nicht in soziale Netze. Gar nicht! Überhaupt nicht!

Abgesehen von der Tatsache, dass es für die Abgebildeten unter Umständen später als Heranwachsende nicht angenehm ist, irgendwo im Internet ein Kinderfoto von sich zu finden, auf dem man komplett eisverschmiert abgebildet ist: Es kann noch weit schlimmer kommen! Immer öfter werden Fälle bekannt, in denen Fotos von Minderjährigen auf pornographischen Seiten auftauchen. Bitte bedenken Sie: Das Internet vergisst nichts. Auch wenn Fotos theoretisch wieder gelöscht werden können: Oftmals bleiben Inhalte auf irgendwelchen Servern erhalten. Daten, die einmal im

Internet gespeichert wurden, können nie mehr vollständig entfernt werden. Das Internet vergisst nie und nichts!

Zum Thema E-Mail: Der Sicherheitsstandard einer unverschlüsselten E-Mail entspricht dem einer Postkarte – also Sicherheitsstandard null!

4. GEBOT

Alexa, Siri & Co. hören mit!

Digitale Sprachassistentinnen sind in Mode und sie können – richtig eingesetzt – tatsächlich eine Hilfe im Alltag darstellen. Natürlich hören sie zu – das sollen sie ja auch. Aber auch hier Vorsicht: Sie könnten auch dann mithören, wenn man das eigentlich nicht beabsichtigt!

Natürlich versichern die Hersteller, dass sich die Spracherfassung nur dann aktiviert, wenn man die virtuellen Helferinnen explizit anspricht. Viele Nutzer haben sich aber auch schon gewundert, dass sich ihre Alexa in ein Gespräch eingeschaltet hat, als zufällig eine Alexandra mit am Tisch saß und Siri reagiert hat, als im Fernsehen eine Dokumentation über Sibirien lief... . Seien Sie sich bitte bewusst, dass die virtuellen Helferinnen auch dann mithören könnten, wenn man das eigentlich gar nicht denkt oder beabsichtigt. Noch immer ungeklärt ist übrigens, wohin Ihre Sprachdaten weitergeleitet werden und ob diese über die Anbieter auch bei Geheimdiensten landen können. Kein Witz!

Denken sie bitte daran, dass man die Sprachassistentinnen ganz einfach manuell deaktivieren kann – denn man braucht sie auch nicht immer!

5. GEBOT

Kinder und Internet – Hüten Sie sich vor Abofallen!

Natürlich bewegen sich auch unsere Kinder im Internet und wie bei den Erwachsenen ist auch bei ihnen manchmal die Versuchung groß: Schnell haben sie an Gewinnspielen teilgenommen, Bestellungen in Online-Shops getätigt oder allerlei Dinge bei eBay ersteigert. Und dann kommt eine Rechnung...

Erster Ratschlag: Sprechen Sie präventiv mit Ihren Kindern und erklären Sie ihnen, dass sie auf keinen Fall an vermeintlichen Gewinnspielen oder Ähnlichem teilnehmen dürfen und dass sie keinesfalls ohne ihre Eltern ihre personenbezogenen Daten irgendwo eingeben dürfen. Vermeiden Sie

von vornherein diesen Ernstfall – dann bekommen Sie auch keine unangenehme Rechnung über drei- oder vierstellige Euro-Beträge... .

Zweiter Ratschlag, wenn es Sie dennoch erwischt haben sollte: Zahlen Sie nicht! Kinder unter 7 Jahren sind nach dem bürgerlichen Recht geschäftsunfähig. Die Vertragserklärung eines Geschäftsunfähigen ist unwirksam. Minderjährige zwischen 7 und 17 Jahren sind hingegen beschränkt geschäftsfähig. Das bedeutet, dass sie grundsätzlich nur mit Einwilligung ihrer Eltern Verträge abschließen können. Eine Ausnahme gilt bei Verträgen, die der Minderjährige mit seinem Taschengeld erfüllen kann. Diese kann er auch ohne Einwilligung seiner Eltern abschließen. Die Eltern sollten nach einem solchen Vertragsabschluss dem Vertragspartner unverzüglich schriftlich mitteilen, dass es sich im Einzelfall nicht um ein Taschengeldgeschäft gehandelt hat und dass sie keine Einwilligung erteilen. Bitte keinesfalls von Mahnschreiben, Drohungen mit Inkasobüros oder sonstigen Druckmitteln beirren lassen!

6. GEBOT

**Einkaufen im Internet –
bitte nur auf sicheren Seiten!**

Es ist ja so verlockend: Ein schon lange, sehlich gesuchter Artikel wird zu einem unschlagbaren Preis in einem Internetshop, den Sie noch nie zuvor wahrgenommen und besucht haben, angeboten. Seien Sie auch da vorsichtig!!

Jedes Mal, wenn Sie online etwas kaufen, müssen Sie natürlich auch bezahlen: Selbstverständlich geben Sie dann Ihre Kreditkartennummer oder Kontodaten an oder überweisen den vereinbarten Betrag per Vorkasse. Da freut sich jeder Internetkriminelle, der Ihre Daten abgreift, weiterverkauft, anschließend Ihr Konto erleichtert und dann im digitalen Nirwana verschwindet – natürlich ohne Ware zu liefern.

Daher: Vertrauen Sie nur Online-Shops, die Sie kennen. Geben Sie Zahlungsinformationen nur auf Seiten ein, die sichere, verschlüsselte Verbindungen bieten. Diese können Sie an der Adresse erkennen. Sie beginnt statt mit http: mit dem Prefix https: . Das „s“ steht hierbei für Secure (also „sicher“). Sichere Adressen werden auch durch ein Schloss-Symbol in der Adressleiste angezeigt.

7. GEBOT

Klicken Sie im Cookie-Banner nicht automatisch auf „Allem zustimmen“!

Mittlerweile kennt sie jeder: Die Cookie-Banner, die Internetseiten erst freigeben, wenn man auf „Zustimmen“ geklickt hat. Das nervt! Aber wissen sie denn auch, wozu sie zustimmen?

Wenn Sie (insbesondere bei Online-Shops) einkaufen, interessiert sich der Betreiber der Seite natürlich nicht nur dafür, Ihnen „nur“ etwas zu verkaufen. Er will mehr über Sie wissen. Er möchte beispielsweise nach Ihrem Besuch in seinem Online-Shop wissen, welche Produkte Sie sich angesehen haben, wie lange Sie welchen Artikel angeschaut haben und noch so manches mehr. Und er registriert die IP-Adresse Ihres Rechners. Mit diesen Informationen wird von Ihnen ein persönliches Kaufprofil erstellt, um Ihnen bei passender Gelegenheit (z.B. in Form eines Newsletters) wieder für Sie passende Angebote zusenden zu können. Aber nicht nur das: Sie stimmen z.B. auch bei der Nutzung von Suchmaschinen (z.B. Google) zu. Damit wird mit Hilfe von „Cookies“ alles gespeichert, was Sie googeln. Damit wissen diese Dienste nicht nur, was sie gerne einkaufen, sondern über Ihr Surf-Verhalten z.B. auch, welche politischen Meinungen Sie haben, an welchen Krankheiten Sie möglicherweise leiden und welche Vorlieben Sie sonst so pflegen. Und man kann Ihren Standort erfassen und von Ihnen ein Bewegungsprofil erstellen.

Aus diesen Gründen hat der Europäische Gerichtshof die Betreiber in seinem „Cookie-Urteil“ verpflichtet, die Nutzer über Cookie-Setzungen zu informieren und ihnen die Möglichkeit zu geben, unerwünschte Cookie-Setzungen zu unterbinden.

Darum: Stimmen Sie nicht blindlings auf allen Cookie-Bannern einfach zu, sondern klicken Sie, wenn immer möglich, zunächst auf „Ablehnen“. Dann wird Ihnen angezeigt, welche Cookies für das Funktionieren der Seite zwingend erforderlich sind und welche zu den oben beschriebenen Folgen führen – und zu diesen verweigern Sie bitte Ihre Zustimmung. Keine Angst: Auch wenn Sie Ihre Zustimmung zu den „kritischen“ Cookies verweigern, funktionieren die Internet-Seiten selbstverständlich und Sie surfen dann um einiges sicherer!

8. GEBOT

**Internet-Rabattportale und Rabattkarten:
Glauben Sie im Ernst an den versprochenen
Benefit?**

Sparen beim täglichen Einkauf ist wichtig – und viele verschiedene Rabattportale, Rabattkarten und Ähnliche versprechen attraktive Nachlässe bei vielen Produkten. Eigentlich ganz gut, aber auch hier ist Vorsicht geboten: Sonst werden Sie

beim Shoppen ganz schnell vom Warenjäger selbst zur gehandelten Ware.

Bevor Sie Ihren ersten Rabatt erhalten, müssen Sie zunächst selber liefern: Nämlich Ihre persönlichen Daten. Sie müssen sich bei allen Anbietern erst einmal registrieren und dabei geben Sie mindestens Ihren Namen, Ihre Anschrift, Ihr Geburtsdatum und Ihre Bankdaten an. Manchmal werden Sie auch noch gefragt, was Sie denn besonders interessiert.

Was harmlos klingt ist es nicht: Die Betreiber erstellen mit diesen Daten ein automatisches Profiling und Scoring (oder auf Deutsch: ein individuelles Persönlichkeitsprofil und eine persönliche Bewertung). So wird zum Beispiel anhand Ihrer Adresse festgestellt, ob Sie (hinsichtlich Ihres Einkommens und Ihres gesellschaftlichen Status) in einem „besseren“ oder „weniger guten“ Viertel leben und gleichzeitig wird im Hintergrund abgeglichen, was bereits bestehende Nutzer in der Nachbarschaft schon alles gekauft haben. Häufig wird auch über eine Abfrage bei der Schufa (für die Sie ohne es zu merken eine Einwilligung erteilt haben) Ihr Einkommen und Ihre Zahlungsmoral erfasst. Insgesamt wird unter Berücksichtigung Ihres Alters so automatisch ermittelt, welche Artikel für Sie interessant sein könnten, was Sie sich finanziell leisten können und ob Sie auch immer sofort zahlen. Dann werden Ihnen über mehr oder weniger subtile Verkaufsmethoden (dazu zählen insbesondere die berühmten Newsletter) bestimmte Artikel bevorzugt angeboten. Wenn Sie nicht im Internet kaufen, sondern vor Ort im Laden wird von ihnen zusätzlich ein Bewegungsprofil erstellt.

Fazit: Statistische Untersuchungen zeigen, dass man mit Rabattsystemen beim Einkaufen zwar sparen kann, dass man aber gleichzeitig auch mehr kauft, weil man permanent dazu animiert wird (wozu gäbe es denn sonst diese Systeme überhaupt?). Und wer profitiert außerdem von Rabattsystemen? Natürlich die jeweiligen (Portal-)Anbieter und fast nur die europa- oder deutschlandweit tätigen großen Ketten, nur selten hingegen der kleine Händler vor Ort (der Ihren Einkauf eigentlich viel mehr verdient und Ihr Geld nötiger hätte). Außerdem liefert man dabei immer seine persönlichen Daten aus. Seien Sie sich dieser Tatsachen bitte immer bewusst.

9. GEBOT

Halten Sie Ihre Antiviren-Software immer auf dem neuesten Stand!

Eigentlich der banalste Hinweis von allen: Internet-Sicherheitssoftware kann Sie nicht vor jeder Bedro-

hung schützen, aber sie erkennt und entfernt die meiste Malware – aber nur, wenn das Produkt auch aktuell ist. Installieren Sie immer schnellstmöglich die neuesten Updates!

10. GEBOT

Verlieren Sie bloß nicht Ihr Smartphone...

... denn es weiß alles über Sie.

Auf unseren Smartphones sind unfassbar viele Daten über uns erfasst: Unser Smartphone weiß, mit wem wir telefonieren, mailen oder whatsappen. Es weiß über die automatische Standorterkennung, wo wir überall waren seit wir das Smartphone benutzen. Es speichert die von uns aufgerufenen Internetseiten und kennt daher auch alle unsere persönlichen Einstellungen und höchstpersönlichen Vorlieben. Wenn wir öfter bestimmte Krankheiten googeln, weiß unser Smartphone auch, woran wir wahrscheinlich leiden. Natürlich kennt es auch alle unsere Kreditkarten- und Kontodaten. Und es kennt unsere Lebensverhältnisse: Es weiß wie wir und unsere Familie und unsere Freunde aussehen, wo wir uns mit ihnen an welcher Stelle des Erdballs getroffen haben und wen wir mögen (oder auch nicht). Es weiß über Ihre installierten Gesundheits-Apps auch, wie viel (oder wie wenig) Sie sich bewegen, kennt Ihre Herzfrequenz und es weiß noch viel mehr... Und jetzt denken Sie bitte darüber nach, was fremde Finder so alles anstellen können... .

Haben Sie schon einmal darüber nachgedacht? Das Smartphone kennt uns besser als wir selbst!

Also: Sichern Sie den Zugriff auf Ihr Smartphone durch den Zugangscode, passen Sie gut darauf auf und verlieren Sie es bitte nicht!

So.....

Jetzt sind wir am Ende unserer „Zehn Gebote“ angelangt. Um ehrlich zu sein: Es gibt noch mindestens 200 weitere. Aber wenn Sie diese zehn Ratschläge berücksichtigen, haben Sie bereits viel erreicht.

Ihr Datenschutzbeauftragter
Martin Brandt
Landratsamt Ostalbkreis

Kontakt: datenschutz@ostalbkreis.de