

WhatsApp, Facebook aber auch berufliche social media wie LinkedIn nicht beruflich nutzen! Sie verletzen ansonsten die DSGVO-Vorschriften!

In den letzten Wochen war in diversen Medien vom Versuch seitens WhatsApp zu lesen, die **Nutzungsbedingungen so zu ändern**, dass die Mutter Facebook Ihre Daten absaugen darf. Die ersten Versuche im Jänner bzw. per 15.5. sind gescheitert, aber sicher nicht der letzte Versuch gewesen.

Auf jeden Fall gilt hier Hände weg von WhatsApp, Facebook und Co.

Aber auch bei der Nutzung beruflicher social media wie etwa **LinkedIn** kommen Sie in Konflikt mit der **DSGVO**.



Im heutigen **9. DSGVO-Praxis-Beitrag** sieht sich der auf Versicherungsrecht und DSGVO spezialisierte Jurist **RA Mag. Stephan Novotny** die Sachlage an und **beantwortet Fragen** wie:

- **Was ist so "böse" an diesen social media?**
- Warum sorgt Apple dafür, dass hier ein **stärkeres Problembewusstsein** entsteht?
- Was sagt der **EuGH zur Nutzung von Facebook?**
- Welche **Entscheidungen** traf der **Datenschutz-Beauftragte Hamburgs** hinsichtlich WhatsApp, Facebook?
- Und **welche Rechte lässt sich z.B. LinkedIn** in seiner Datenschutzerklärung **von Ihnen einräumen?**

Die **bisher erschienenen Praxis-Beiträge zur DSGVO** von **Mag. Novotny** beschäftigten sich mit folgenden Themen:

DSGVO 1: DSB-Urteil zur **maximalen Speicherdauer**: Wie Freibeweisen ohne Unterlagen? [Hier weiterlesen...](#)

DSGVO 2: **TOMs**: Was lernen wir aus **Megastrafe**? [Hier weiterlesen...](#)

DSGVO 3: **Ausweiskopien**: Nie unverändert speichern oder versenden! [Hier weiterlesen...](#)

DSGVO 4: **Millionenstrafe wegen telefonischer Auskunft!** Was lief schief? Wie besser machen? [Hier weiterlesen...](#)

DSGVO 5: Was fordert **EuGH zur Einwilligung bei Cookie-Nutzung** auf **Webseite**? Abmahnungen vermeiden! [Hier weiterlesen...](#)

DSGVO 6: Rückblick auf Datenschutz-Urteile 2020. [Hier weiterlesen...](#)

DSGVO 7: Teil2: Wann und wie darf man **Kunden und Interessenten** seit Wirksamkeit der DSGVO **noch kontaktieren**? [Hier weiterlesen...](#)

DSGVO 8: **Datenpanne: Zu viele Mail-Adressen** unter AN oder CC: Was ist zu tun? [Hier weiterlesen...](#)

WhatsApp, Facebook aber auch berufliche social media wie LinkedIn nicht beruflich nutzen! Sie verletzen ansonsten die DSGVO-Vorschriften!

Hände weg!

Bereits im Jänner und dann per Stichtag 15.5. gab es erste Versuche (waren sicher nicht die letzten) seitens WhatsApp, die Nutzungsbedingungen derart zu verändern, dass auch die „Mutter Facebook“ auf alle Daten zugreifen und für Werbezwecke nutzen darf.

Diese Versuche gingen schief. Nicht nur eingefleischte Datenschützer, die bereits seit Jahren vor Facebook und WhatsApp warnen, schrien auf. Sondern auch zahlreiche Medien und Foren berichteten darüber, sodass einiger Widerstand der Nutzer entstand. Und viele etwa zu „Signal“ oder „Threema“ wechselten, die nicht auf die Daten der Nutzer „scharf sind“.

„Kurioserweise“ ist es Apple zu verdanken, dass hier Problembewusstsein geschaffen wurde. Denn Apple zeigt seit einigen Wochen an, welche Daten eine App von Ihrem Gerät absaugt. Und das ist eben bei WhatsApp und Facebook erschreckend viel und erlaubt das Erstellen von Nutzerprofilen, die Sie besser kennen, als Sie sich selbst! **Eine eindrucksvolle Graphik welche Daten weiter geleitet werden, finden Sie unten.**

Daher kann man nur warnen, keinesfalls diesen geänderten Nutzungsbedingungen zuzustimmen, weil Sie dadurch WhatsApp die Erlaubnis geben, alle Ihre Daten zu kopieren, zu transferieren, zu Werbe- oder sonstigen Zwecken zu nutzen. Ganz nach dem **Motto: Sie sind nicht der Kunde, sondern die Ware!**

Interessanterweise löste die Ankündigung von WhatsApp – **wer nicht zustimme, könne WhatsApp nach dem 15.5. nicht mehr nutzen**, heftigen Gegenwind aus. Man las sogar von Erpressung im Netz: So schieb etwa Campact: „Das Unternehmen erpresst die WhatsApp-Nutzer*innen regelrecht: Wer bis zum 15. Mai den neuen Bedingungen für die weit verbreitete App nicht zustimmt, kann keine Nachrichten mehr lesen oder schreiben...“ und man **zitierte Hamburgs Beauftragten für Datenschutz, Johannes Caspar**, der über die Pläne entsetzt sei und einen rechtswidrigen massenhaften Datenaustausch befürchtet(e).

Und weiter: „Der Online-Gigant verlangt einen Blankoscheck. **Wer die App weiter nutzen will, muss seine Daten unbegrenzt allen Facebook-Unternehmen zur Verfügung stellen.** Was genau der Konzern damit anstellen will, verrät er aber nicht. „Vage und widersprüchlich“ sei Facebooks Datenschutzrichtlinie, so Caspar – und „möglicherweise rechtswidrig“.

Zur besseren Einordnung: In Deutschland gibt es keine zentrale Datenschutzbehörde, sondern jedes Bundesland hat eine eigene! Daher lesen Sie wie oben von einem **Datenschutz-Beauftragten Hamburgs oder der Bayrischen Datenschutzbehörde** (BayLDA), etc. Diese Ämter sind **mit unserer Datenschutzbehörde** vergleichbar und kämpfen überaus aktiv um die Einhaltung der Datenschutzgrundverordnung, kurz DSGVO. Und obiger **Datenschutzbeauftragter Caspar** traf dann einige Tage später eine Entscheidung und **hat Facebook verboten, Daten von WhatsApp zu verarbeiten.**

Wie kam er zu dieser Entscheidung?

Es liegen zumindest **2 Entscheidungen des Europäischen Gerichtshofes vor**, die feststellen, dass Sie sowohl beim Setzen von Social Plugins (also etwa den **Einbau eines Facebook Like Button** auf der eigenen Webseite), aber auch die Erstellung und **Nutzung von Facebook-Fanpages** (also Webseiten auf Facebook) **die gemeinsame Datenverantwortung mit Facebook** haben. Das bedeutet, dass Sie genauso für die missbräuchliche Nutzung der Daten durch Facebook und Co mitverantwortlich sind und geklagt/ bestraft werden können.

Ein praktisches Beispiel: Wenn Sie eine eigene Seite auf Facebook betreiben, hat das zur Folge, dass alle Personen, die diese Fanpages aufrufen, genau dadurch von Facebook getrackt werden. Somit sind sie allen Nutzern ihrer Fanpage datenschutzrechtlich genauso verantwortlich wie Facebook. Aber Sie wissen natürlich nicht, was Facebook wirklich mit den Daten tut....

Ich muss kein großer Prophet sein, um vorherzusagen, dass Sie keinen Einfluss auf Facebook und die Rahmenbedingungen haben, die Ihnen Facebook für Ihre Unternehmensseite zur Verfügung stellt. So lässt sich etwa **Facebook Insights** und das damit einhergehende Tracking der Seitenbesucher nicht deaktivieren.

Der oben zitierte **Datenschutzbeauftragte der Stadt Hamburg, riet nach Veröffentlichung des zitierten EuGH-Urteils:** „Sie müssen von Facebook nun sowohl die volle Transparenz über die Verarbeitung der Nutzerdaten in diesem Zusammenhang gegenüber den Fanpage-Besuchern einfordern und, insoweit diese mit geltendem Datenschutzrecht nicht vereinbar ist, Änderungen durch Facebook erwirken oder das Angebot beenden.“ Viel Glück kann man da nur wünschen....

Und das war im Juni 2018, also noch lange vor dem **Ende des Privacy Shield Abkommens mit den USA**, seither ist der Datenaustausch zwischen EU und USA sowieso verboten.

Zum Nachlesen zu dieser Problematik empfehle ich:

- <https://datenschutz-hamburg.de/pages/search/?s=facebook>
- <https://datenschutz-hamburg.de/pressemitteilungen/2018/06/2018-06-05-eugh-fanpages>
- <https://datenschutz-hamburg.de/pressemitteilungen/2018/03/2018-03-02-oberverwaltungsgericht-best%C3%A4tigt-verbot-des-datenaustauschs-zwischen-whatsapp-und-facebook>
- http://curia.europa.eu/juris/document/document_print.jsf;jsessionid=396D10847F7AAE7156AA422B3792E4C6?docid=216555&text=&dir=&doclang=DE&part=1&occ=first&mode=DOC&pageIndex=0&cid=2187223

Nochmals meine Botschaft:

WhatsApp, Facebook und Co, aber auch berufliche Social Media wie etwa LinkedIn (gehört zu Microsoft) nicht beruflich nutzen!

Denn: Wenn Sie WhatsApp nutzen, verstoßen Sie in mehrfacher Weise gegen die DSGVO. Zur Erinnerung: Wir sind durch die DSGVO verpflichtet, **die Daten der Partner, Kunden, etc. zu schützen** und dürfen diese **keinesfalls an Dritte (hier eben an Facebook) weiterleiten.**

Denn dazu haben Sie vorab **keine Zustimmung durch Ihre Kontakte, Kunden, Partner, etc. erhalten!**

Daher: Hände weg von Social Media-Tools im Geschäftsbereich.

Aber was soll ich nun tun?

Keine Sorge: Es gibt genug Alternativen zu WhatsApp. Datenschützer präferieren beim Thema Messenger seit Jahren „Signal“. Aber auch Threema wird sehr empfohlen, da dies ein Europäischer Messenger ist.

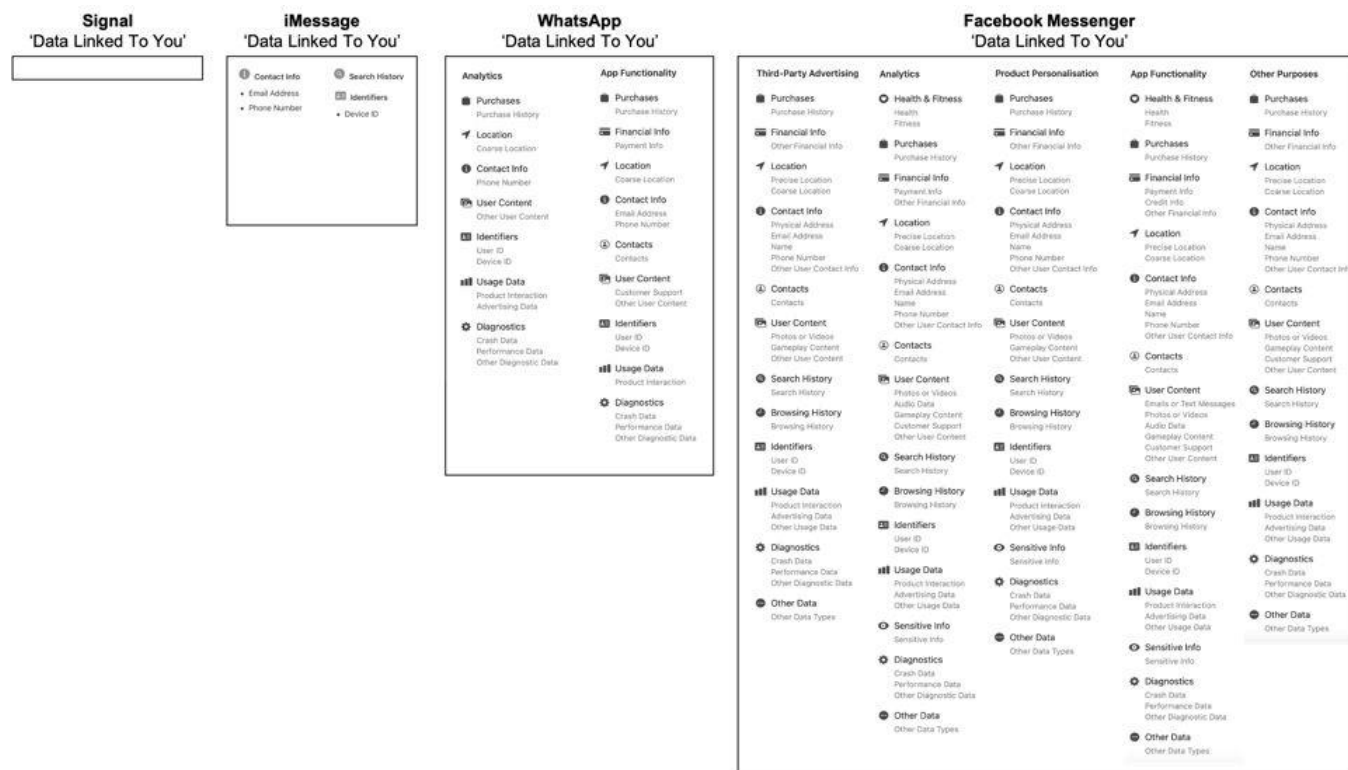
Aber es gibt auch zahlreiche andere Messenger-Alternativen. Einfach Ihren EDV-Betreuer fragen oder bei anerkannten Computer-Zeitungen nach Messenger-Tests suchen:

Lesetipp: https://www.chip.de/news/Die-besten-Messenger-Es-muss-nicht-immer-WhatsApp-sein_118989233.html

Tipp: Die oben angesprochene „Apple-Transparenz-Offensive“ zeigt ganz klar, dass **SIGNAL** (in der folgenden Graphik ganz links) keine persönlichen Daten sammelt.

Facebook (ganz rechts) aber fast alles... Und WhatsApp ist auch nicht bescheiden:

Die folgende **übersichtliche Graphik von FORBES** zeigt die **Sammelwut** ganz deutlich:



Nach WhatsApp und Facebook, kommt meist die folgende Frage: **Wie sind berufsorientierte social media wie etwa XING oder LinkedIn im Hinblick auf die DSGVO zu sehen?**

Haben Sie auch hier Datenschutzbedenken?

Meine Antwort: Zu diesen berufsorientierten social media findet meiner Wahrnehmung nach noch **kaum eine Datenschutz-Diskussion** statt. Trotzdem es auch hier Datentransfers gibt – möglicherweise sogar in die USA (was nach dem Auslaufen des Privacy Shield-Abkommen Gefahrenpotential birgt).

Das liegt wohl daran, dass man bei den „privaten“ social media **lange nicht damit rechnet**, dass es zum Absaugen von Daten und Kontakten kommt. Und man durch Nutzung der social media zum „**Gläsernen Menschen**“ wird. Was zur Folge hat, dass die Werbetreibenden ganz genau wissen, welchen Flug man unbedingt kaufen möchte (damit steigt der Ticketpreis), wie es mit der Kreditwürdigkeit aussieht (und man dadurch keinen Handy-Vertrag oder Kredit bekommt) und und und. Von der Möglichkeit via Facebook Wahlen entscheiden zu können, konnte man sich bei der Brexit-Abstimmung und der Wahl Donald Trumps erste Reihe fußfrei überzeugen. Doch schön langsam wächst bei vielen Menschen das Problembewusstsein. Und man versteht, dass diese Produkte deshalb kostenlos zu nutzen sind, **weil man selbst und die Daten der auf den Geräten gespeicherten Kontakten die eigentliche Ware geworden** sind, mit der die Datenkraken ihr Milliarden-Geschäft machen. Und dadurch finden in letzter Zeit – auch ausgelöst durch das Inkrafttreten der DSGVO – Datenschutz-Diskussionen bei Nutzung von Facebook, WhatsApp und Co statt.

Bei beruflichen social media konnte ich auch trotz Recherche kaum solche Diskussion finden. Auch auf diversen Webseiten von verschiedenen Datenschutzbehörden und – beauftragten (siehe etwa obige Links zum Datenschutzbeauftragten Hamburgs, der sehr aktiv informiert) findet sich kaum etwas.

Ich vermute, das liegt daran, dass **alle Beteiligten sich klar sind**, dass die eigenen Daten gesammelt, geteilt, etc. werden. Dennoch gilt, **Sie haben nicht die Zustimmung von allen Ihren Kontakten erhalten**, dass deren Daten, etc. an Microsoft weitergeleitet und zu Nutzerprofilen verarbeitet und für Werbezwecke verwendet werden dürfen.

Liest man die **Datenschutzerklärung z.B. von LinkedIn** - [hier zum Nachlesen](#) - steht alles ganz klar da:

- > Weitergabe und Verarbeitung der eigenen Daten (Punkt 1 der DS-Erklärung),
- > Weitergabe der Kontakt- und Kalender Daten (Punkt 1),
- > Verknüpfung mit Daten von „verbundenen Unternehmen und Diensten“ (Punkt 1.2, da wird z.B. ausdrücklich Microsoft und deren Produkte genannt), Protokollierung der Nutzungsweise und Speicherung (Punkt 1.3 erwähnt Nutzung, Cookies, Geräteinformationen, IP-Adressen...),
- > Speicherung der Webnutzung (Punkt 1.5 Navigieren durch Netz, welche Seiten Sie ansehen, IP-Adresse, Betriebssystem, Geräteerkennung und –funktionen, Ihre Cookie-ID (Anmerkung: Damit werden Sie auch von anderen Werbepartnern erkannt, selbst wenn Sie glauben anonym durchs Netz zu surfen),
- > Analyse Ihrer Nachrichten (Punkt 1.6: „wenn Sie mit unseren Diensten Nachrichten senden, erhalten oder interagieren)
- > Webseiten und Dienste Dritter (Punkt 1.8: „erhalten Daten, wenn Sie Webseiten besuchen...“

Also alles da, um Sie und Ihre Kontakte ganz genau kennenzulernen.

Und weiter zu geben, Details siehe Punkt 2.4.:

Zwar beginnt der Satz positiv, dass nämlich „personenbezogene Daten nicht an dritte Werbetreibende oder Anzeigennetzwerke“ weitergeleitet würden. Doch dann folgen die Ausnahmen: IDs, Gerätekennungen; Daten, die bereits jedem zugänglich sind (also Ihre Profildaten), usw.

In Punkt 3.3 bestätigen Sie was alles mit Diensten Dritter passiert („können andere Dienste Ihr Profil aufrufen“.

In Punkt 3.4 erfahren Sie, dass LinkedIn „Ihre Daten über unsere verschiedenen Dienste und mit LinkedIn verbundenen Unternehmen“ teilt und „zusammenführt, um unsere Dienste für Sie und **andere** relevanter und nützlicher zu gestalten“.

Das ist schon sehr deutlich! Dennoch habe ich das Wort andere fett gesetzt, um zu zeigen, dass nicht nur Sie im Mittelpunkt stehen, sondern man auch andere Interessen verfolgt.

Punkt 5.2. erlaubt den **landesübergreifenden Datentransfer**: „Wir verarbeiten Daten sowohl innerhalb als auch außerhalb der USA“. Das ist angesichts des **Endes des Datashield-Abkommens zwischen EU und USA** nicht unerheblich. Bedenken Sie: Die Anforderungen an Datenschutz sind in den USA nicht mit jenen in Europa vergleichbar. Überhaupt, wenn es sich um die Daten von Europäern handelt!

Wer sich also die Mühe macht, die Datenschutzerklärung von LinkedIn zu lesen, darf nicht überrascht sein, was mit seinen eigenen Daten und Daten seiner auf dem Gerät gespeicherten Kontakten gemacht wird.

Und erst kürzlich schlagzeilte DER STANDARD:

Daten von 500 Millionen LinkedIn-Nutzern werden im Netz verkauft. Zum Lesen [hier klicken...](#)

LinkedIn und Microsoft (denen LinkedIn gehört) betonen zwar, dass man nach jetzigen Wissenstand glaube, dass es keine Lücke und keinen Hackerangriff gebe, sondern die von den Nutzern freiwillig zur Verfügung gestellten Daten seien einfach über die Jahre kopiert worden. Meiner Ansicht nach nicht beruhigend. Und man könnte nun sagen: Vorher überlegen, auf welchen Plattformen man welche Daten veröffentlicht!

Denn dumm ist nun, **dass man mit diesen persönlichen Daten** (Name, Adresse, Telefonnummer, Details zum Beruf, etc.) sehr viel Unsinn anstellen kann, der teuer werden kann.

So gibt es durch ein bekanntgewordenes **Facebook-Datenleck** (Daten von 500 Mio. Facebook-Nutzern werden im Netz angeboten, Stand 8.4.) seit Wochen **eine SMS-Spamwelle weltweit**, weil eben auch die Telefon-Nummern gestohlen wurden.

In diesen SMS wird dann behauptet, dass ein Paket nicht zugestellt werden konnte, dass eine Überweisung oder eine Bestellung bei diversen Portalen nicht ausgeführt werden konnte (siehe aktuelle Warnung betreffend Willhaben-SMS bei Watchlist Internet) und ähnliches mehr. Ziel dieser SMS ist, dass die Empfänger auf einen Link klicken, um das Problem zu beheben. Man landet dann auf gefälschten Webseiten von DHL, Willhaben, Banken, usw., wo dann weiterer Datenverlust oder sogar finanzielle Verluste drohen.

Tipp: Um zu prüfen, ob man von einem dieser Datenhacks betroffen ist, empfehlen Datenschützer die Seite <https://haveibeenpwned.com/> .
Dort können Sie prüfen, ob Ihre E-Mail-Adresse - oder seit neuestem – Ihre Telefonnummer bei einem Hack gestohlen wurde.

Abschließend: Noch findet keine Datenschutz-Diskussion bei diesen beruflichen social media statt. Aber angesichts der Berechtigungen, die man diesen Tools gibt (siehe oben), ist es meiner Ansicht nach nur eine Frage der Zeit, bis das auch hier eintreten wird.

Ich kann also auch bei diesen beruflichen social media nur warnen und abraten.

Denn auch im beruflichen Kontext haben Sie nicht die Zustimmung vom Kunden erhalten, seine Daten weiterzugeben. Es ist bei LinkedIn kaum ein Unterschied zu WhatsApp zu erkennen.

Auch wenn es manche – noch – nicht hören möchten: Hände weg von social media im beruflichen Zusammenhang.

Quellen: Webseite des Datenschutzbeauftragten der Stadt Hamburg, Campact.de, Chip.de, DerStandard.at, Webseite IVVA.at, Datenschutzerklärung von LinkedIn

beste Grüße von Mag. Stephan Novotny und Günter Wagner

Alle bisherigen IDD und DSGVO-Praxisbeiträge können Sie [hier herunterladen...](#)
Den aktuellen Beitrag können Sie als PDF anfordern. Dazu einfach ein E-mail an g.wagner@b2b-projekte.at mit Betreff "Ja zu Infos".

Für Rückfragen:

MAG. STEPHAN M. NOVOTNY



Rechtsanwalt-Attorney at Law / Akademischer Versicherungskaufmann
/ Collaborative Law Lawyer

Weihburggasse 4/2/26, A-1010 Wien

Tel: +43 / 1 / 512 93 37,

Fax +43 / 1 / 512 93 37 93, Mob. +43 / 664 / 143 29 11

kanzlei@ra-novotny.at www.ra-novotny.at