Aktuelle Fragen zur EU-Datenschutz-Grundverordnung

Antworten auf die wichtigsten Fragen

1. Muss ich meine Facebook-Unternehmensseite („Fanpage“) „schließen“?

Nein, es gibt nur Adaptierungsbedarf. Der Europäische Gerichtshof (EuGH) hat in einem medial sehr stark thematisierten Urteil dargelegt, dass Betreiber von Facebook-Fanpages mit Facebook gemeinsam „Verantwortliche“ sind. Das mag auf den ersten Blick erschrecken oder überraschen, es gibt jedoch ein paar Dinge dazu zu sagen:

Im Urteil ist an keiner Stelle dargelegt, dass Fanpages geschlossen werden müssen, dh gelöscht werden müssen.

Es ist sehr ratsam (und daher keine Neuerung), auch auf der Facebook-Fanpage ein Impressum und eine Datenschutzerklärung anzubieten (oder zumindest auf jene der eigenen Website direkt zu verlinken) um darzulegen, welche personenbezogene Daten vom Betreiber der Fanpage verarbeitet werden. Hier ist auch über allfällig gesetzte Cookies zu informieren. Bei der „gemeinsamen Verantwortlichkeit“ (vgl EU-Datenschutz-Grundverordnung (DSGVO): Pflichten des Verantwortlichen) sollte mit Facebook zusammengearbeitet werden, da Facebook über die notwendigen Informationen hierüber verfügt. Das Soziale Netzwerk arbeitet bereits daran und hat einen sogenannten „Artikel 26 DSGVO – Vertrag“ bereitgestellt, der bei der Erstellung von Fanpages akzeptiert werden muss (vgl Seiten-Insights-Ergänzung bezüglich des Verantwortlichen). Zwar ist dieser nicht perfekt, aber immerhin ein erster Schritt.

Wann und unter welchen Umständen Cookies gesetzt werden dürfen, ist nicht direkt durch die EU-Datenschutz-Grundverordnung (DSGVO), sondern in Österreich durch das Telekommunikationsgesetz (TGK) geregelt. Das Abspeichern von Cookies auf dem Endgerät des Kunden, um Daten mit dem Computer des Kunden zu verknüpfen, ist in Österreich zulässig, wenn die Einwilligung des Users eingeholt wurde und der User entsprechend informiert wurde. Die Einwilligung kann auf verschiedenen Wegen eingeholt werden, z.B. in diesem Fall auch durch Facebook selbst. Dh folgende Adaptierungen sind durchzuführen oder ggf zu ergänzen:

- es muss ein Impressum auf der FB-Seite angeführt werden,
- es muss eine DS-Erklärung ausgewiesen werden,
- in der DS-Erklärung sollte jedenfalls und nach wie vor über die Datenverarbeitung via Facebook informiert werden (eine nähere Beschreibung):
    - rechtliche Grundlage (z.B. Art 6 Abs 1 lit f DSGVO)
    - welche Daten werden Facebook erhalten und wie werden diese genutzt (z.B. statistische Daten unterschiedlicher Kategorien wie Gesamtzahl von Seitenaufrufen, „Gefällt mir“-Angaben, Seitenaktivitäten, Beitragsinteraktionen, Videoansichten, Beitragsreichweite, Kommentare, Geteilte Inhalte, Antworten, Anteil Männer und Frauen, Herkunft bezogen auf Land und Stadt, Sprache, Aufrufe und Klicks im

Shop, Klicks auf Routenplaner sowie Klicks auf Telefonnummern)
- wofür werden diese Daten genutzt
- bestenfalls auch eine direkte Verlinkung auf die DS-Erklärung von Facebook selbst: https://www.facebook.com/about/privacy/
- gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO und Verweis bzw Verlinkung auf das Page Controller Addendum

2. Ich habe gelesen, dass die Europäische Kommission ein „Vertragsverletzungsverfahren" gegen Österreich überlegt, angeblich wurde die DSGVO hier aufgeweicht. Was heißt das für mich im Unternehmen?

Im Moment nichts. Es wurden von der Europäischen Kommission Bedenken zum Datenschutz-Deregulierungs-Gesetz 2018 geäußert, bisher gibt es aber noch keine Entscheidung. Bei den wirtschaftsrelevanten Bereichen (Beraten statt Strafen, Ausnahmen vom Auskunftsrecht bei der Gefährdung von Geschäfts- und Betriebsgeheimnissen), sind die Spielräume genutzt worden, die die DSGVO selbst gegeben hat. An der Umsetzung in den Betrieben hat das österreichische Gesetz nichts geändert.

3. Ich erhalte auch jetzt noch (nach dem 25. Mai 2018) täglich mehrere E-Mails mit „Neue Datenschutzbestimmungen" oder „Datenschutzerklärungen". Was soll ich damit?

Wenn Sie mit dem Unternehmen in Kontakt waren (z.B. Vertragsabschluss, eine aufrechte Kundenbeziehung, Sie haben sich einmal zum Newsletter angemeldet, ...), ist das grundsätzlich etwas Positives. Die Unternehmen wollen Sie darüber aufklären, was Sie mit Ihren Daten machen – warum sie diese haben, wohin diese geschickt werden etc. Da Datenschutz ein sehr wichtiges Thema wurde, wollen Unternehmen auch zeigen, dass Ihre Daten Ihnen wichtig sind.

> **Achtung:** Prüfen Sie dennoch jedes E-Mail, das Sie erhalten. Kennen Sie den Absender? Stimmt der Absender auch mit dem Unternehmen, von dem es vermeintlich geschickt wurde, überein?

4. Wenn jemand meinen Newsletter nicht mehr will (z.B. ist dieser abbestellt worden), was muss ich tun?

Sie dürfen in einem solchen Fall dem jeweiligen Empfänger keine elektronischen Nachrichten zu Werbezwecken mehr schicken, dh Sie müssen sicherstellen, dass er bei der nächsten Newsletter-Aussendung nicht mehr in Ihrem Mailverteiler aufscheint. Ob Sie die E-Mail-Adresse generell löschen müssen, hängt davon ab, ob Sie diese noch aus anderen Gründen (nicht mehr Newsletter-Versand) benötigen (z.B. um einen Vertrag erfüllen zu können). Wenn das nicht der Fall ist, sollten Sie die E-Mail-Adresse auch löschen (vgl Aufbewahrungsfristen / Löschung).

5. Ich habe in der Zeitung gelesen, dass die Datenschutzbehörde auch Einwilligungserklärungen sehr stark überprüft. Was muss ich hier ändern?

Sie sollten 1. prüfen, ob Sie überhaupt eine Einwilligungserklärung brauchen oder ob Sie die Datenverarbeitung auf eine andere Grundlage stützen können (z.B. Vertrag, Gesetz, berechtigtes Interesse,... vgl EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung). Wenn Sie eine Einwilligung benötigen, dann prüfen Sie als 2. Schritt, ob Sie alle notwendigen Punkte eingehalten haben (freiwillig, konkret, auf den Einzelfall bezogen, verständlich formuliert, nicht in anderen Vertragsbedingungen versteckt uÄ, vgl EU-Datenschutz-Grundverordnung (DSGVO): Einwilligungserklärung) .

6. Wohnhausanlage – Namensschilder bei Gegensprechanlage

Gemeindewohnungen in Wien werden aufgrund einer Datenschutz-Beschwerde eines Mieters, dessen Namensschild an der Türklingel bei der Gegensprechanlage ausgewiesen wurde, alle Klingelschilder gegen Türnummern austauschen. Diese Entscheidung wurde von der zuständigen Magistratsabteilung der Stadt Wien getroffen. Eine Entscheidung der Datenschutzbehörde selbst ist offenbar nicht getroffen bzw gar verlangt worden (so im Ö1 Mittagsjournal vom 12. Oktober).

Datenschutz gibt es nicht erst seit dem 25. Mai 2018, auch zuvor bestanden schon (strenge) datenschutzrechtliche Regelungen in Österreich. Namensschilder bei Türen wurden teilweise aufgrund von ausdrücklichen Einwilligungen (Ankreuzmöglichkeit beim Mietvertrag / separate Unterschrift), schlüssigen Einwilligungen oder auch aufgrund von „berechtigten Interessen" angebracht. Auch mit der EU-Datenschutz-Grundverordnung (DSGVO) hat sich hier keine Änderung ergeben. Dh sofern nicht die Interessen der betroffenen Person überwiegen, ist es nach wie vor möglich, mit berechtigten Interessen des Datenschutz-Verantwortlichen oder von Dritten zu argumentieren. Auch Einwilligungen (ausdrücklich oder schlüssig) sind nach wie vor zulässig. Es liegt noch keine anderslautende Entscheidung der Datenschutzbehörde vor. „Berechtigte Interessen" könnten im Fall Türschilder mit verschiedenen Beispielen argumentiert werden, zB Einsatzfahrzeuge müssen rasch und oftmals in akuten Notsituationen Wohnungen auch mit möglicherweise schlechterer Adressbeschreibung aufsuchen; Post- oder Paketzusteller erhalten fehlerhafte Adressen, etc. Es kommt nach der DSGVO darauf an, was Personen vernünftigerweise erwarten können. Im Rahmen eines Mietvertrags- aber auch Verwaltervertragsverhältnis wird üblicherweise

auch bisher davon ausgegangen worden sein, dass Namen der Bewohner auch bei Türschildern oder Klingelanlagen angebracht werden. Nach der Gewerbeordnung müssen Gewerbetreibende sogar zur äußeren Kennzeichnung der Betriebsstätte den Namen anführen.

Es wäre aber möglich, dass sich eine betroffene Person an den Verantwortlichen wendet und einen Widerruf ihrer Einwilligung oder einen Widerspruch wegen „höherwertiger" Interessen einlegt, dh verlangt, dass die Daten nicht (mehr) offengelegt werden. Das ist offensichtlich im Fall der Gemeindewohnungen passiert. Der Betreiber hat sich daher nun dazu entschlossen, eine einheitliche Lösung zu finden und sich für diesen Weg entschieden. Die Mieter haben lt Presseberichten nach wie vor die Möglichkeit, selbst das Schild gegen ein Namensschild einzutauschen. Diese Lösung ist risikolos, jedoch nicht die einzig gangbare. Wer sich nicht mit Interessenabwägungen („berechtigte Interessen") befassen und auf Nummer sichergehen will, kann sich zB auch bei Mietvertragsabschlüssen bestätigen lassen, was am Klingelschild ausgewiesen sein soll (zB separates Kästchen im Mietvertrag). Möglich wäre auch, die Mieter/ Eigentümer anzuschreiben und um Einwilligung („bis zum…") zu fragen – wenn diese bis zum Stichtag nicht erhalten wird, sollte das Türschild aber abmontiert werden (Schweigen gilt nicht als Einwilligung).

7. Warum gilt der Steuerberater nicht mehr als Auftragsverarbeiter?

Das ist eine gute Frage. Wir haben uns als WKO immer auf eine bereits ergangene Entscheidung der Datenschutzbehörde gestützt, ebenso wie auf die Stellungnahme der Artikel 29 Gruppe zu Auftragsverarbeitern und Verantwortlichen aus 2010 (wp169 DE Verantwortlicher Auftragsverarbeiter). Nun gibt es seit Jänner (veröffentlicht im April) eine neue Entscheidung der DSB zu diesem Thema (DSB-D122.767/0001-DSB/2018). Diese Entscheidung argumentierte neu und ließ den bisherigen Bescheid aus 2005 (K120.862/0011-DSK/2005) unkommentiert. Da es sich um eine neue Entscheidung handelt, wird auch diese im Moment zitiert und übernommen.

Achtung: Auch diese Information könnte jederzeit wieder „alt" sein, da wie bereits erwähnt, es sich lediglich um eine Entscheidung in der 1. Instanz handelt. Es gibt zu dieser Problematik noch keine Entscheidung der österreichischen Verwaltungsgerichte und noch keine des Europäischen Gerichtshofs. Datenschutz ist kein starres Thema („Der 25. Mai ist vorbei, jetzt ist alles fertig"), es wird sich ständig Neues ergeben, auf das geachtet werden muss**. Meinungen/Auslegungen können auch revidiert werden!**

8. Update WhatsApp

Wieder hat eine deutsche Datenschutzstelle eine Empfehlung bzw eine Fragebeantwortung zum Thema „WhatsApp" aufgenommen. Im Newsletter des DSBA von Rheinland-Pfalz wurde folgendes ausgewiesen: „Darf ich mit den Eltern über E-Mail oder WhatsApp kommunizieren?"

Allgemeine Hinweise, Einladungen zu Veranstaltungen etc. sind auch per E-Mail möglich. Persönliche Daten in Bezug auf einzelne Kinder sollten per Mail nicht unverschlüsselt versendet werden.

Beachten Sie: Eine unverschlüsselte E-Mail gleicht vom Sicherheitsniveau her einer Postkarte. Die Nutzung privater Endgeräte, wie Smartphones und Tablets, für dienstliche Zwecke sollte nur in Absprache mit der Kitaleitung erfolgen. Sofern es als notwendig erachtet wird, über Messenger mit Eltern zu kommunizieren, kommen nur europäische Anbieter, die eine Ende-zu-Ende-Verschlüsselung anbieten, in Betracht (z. B. Pidgin/OTR, Signal 2.0, SIMSme, Chiffry, Signal, Threema oder Wire).

Die Nutzung von WhatsApp ist daher für dienstliche Kommunikation nicht zulässig. Dort werden die Daten auf Servern verarbeitet, die in rechtlicher und technischer Hinsicht nicht europäischem Datenschutz-Standard entsprechen. Sie unterliegen einem unkontrollierten Zugriff durch US-amerikanische Stellen."

9. Ich habe gehört, dass ich jetzt auch über 50 Empfängern E-Mails zu Werbezwecken verschicken darf, stimmt das?

Nein! E-Mails zu (Direkt-)werbezwecken unterliegen sehr strengen Vorgaben (vgl auch die FAQ Newsletter-Versand), das bereits ab der ersten elektronischen Nachricht. „Spamming" ist nach wie vor (außer in speziellen Ausnahmen, vgl Newsletter-Versand) verboten, allerdings besteht eine kleine Erleichterung für E-Mails, welche nicht zu Direktwerbezwecken versendet werden. Hier ist die ominöse 50 Mail Grenze (Massensendung) gefallen. Direktwerbung wird von der Rechtsprechung weit ausgelegt und erfasst jeden Inhalt, der für ein bestimmtes Produkt, eine bestimmte Idee, bestimmte politische Anliegen wirbt oder Argumente liefert (Beispiele für Direktwerbung: Abfrage eines gewissen Verbraucherverhaltens, Kundenzufriedenheitsanfragen). Markt- und Meinungsforschung gilt dann nicht als Direktwerbung, wenn diese nicht dem Ziel dient, unmittelbar oder mittelbar den Absatz eines Unternehmens zu fördern.

Außerdem müssen allgemeine Anforderungen bei der Zulässigkeit der Werbemails eingehalten werden:

- die Identität des Absenders, in dessen Auftrag die Nachricht übermittelt wird, darf nicht verschleiert oder verheimlicht werden,
- die Bestimmungen des § 6 Abs 1 E-Commerce-Gesetz müssen eingehalten werden, d.h.
    - kommerzielle Kommunikation muss als solche erkennbar sein und
    - die natürliche oder juristische Person, die die kommerzielle Kommunikation in Auftrag gegeben hat, muss sich zu erkennen geben,
    - Angebote zur Absatzförderung wie etwa Zugaben und Geschenke müssen als solche erkennbar sein und einen einfachen Zugang zu den

Bedingungen für ihre Inanspruchnahme enthalten und
    - Preisausschreiben und Gewinnspiele müssen als solche zu erkennen sein und einen einfachen Zugang zu den Teilnahmebedingungen beinhalten
- der Empfänger darf nicht aufgefordert werden, Websites zu besuchen, die gegen § 6 Abs 1 E-Commerce-Gesetz verstoßen oder
- in denen keine authentische Adresse vorhanden ist, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

D.h. die Erleichterung, die mit der Telekommunikationsgesetz-Novelle 2018 einherging, betrifft Newsletter und „normale Werbemails" leider **nicht**.

10. EU-US Privacy Shield ist nicht mehr gültig

> Der **Europäische Gerichtshof (EuGH) hat am 16. Juli 2020 das EU-US Privacy Shield mit sofortiger Wirkung für ungültig erklärt** (Urteil in der Rechtssache C-311/18 Data Protection Commissioner / Maximillian Schrems und Facebook Ireland, vgl Pressemitteilung des EuGH).

Was ist das EU-US Privacy Shield?

Das EU-US Privacy Shield ist ein Abkommen zwischen der EU und den USA, welches die Übermittlung personenbezogener Daten von der EU in die USA regelte. Mit dem Privacy Shield sollte ein Nachfolger für das vorherige Abkommen, Safe Harbor, gefunden werden, das bereits 2015 vom Europäischen Gerichtshofs (EuGH) für ungültig erklärt wurde („Urteil Schrems I").

Dieses Abkommen ist eine sogenannte „Angemessenheitsentscheidung", mit der festgestellt wird, dass die USA ein EU-konformes Datenschutzniveau für den Datentransfer aus der EU an US-Unternehmen, die sich diesem „Privacy Shield" unterwerfen, gewährleisten. US-Unternehmen hatten die Möglichkeit, sich in eine vom US-Handelsministerium geführten Liste („Privacy Shield List") eintragen zu lassen, wenn sie sich zur Einhaltung der vereinbarten verbindlichen Anforderungen („Privacy Shield Principles") durch eine Selbstzertifizierung gegenüber dem US-Handelsministerium verpflichten.

Was ist passiert?

Max Schrems, ein österreichischer Datenschutzaktivist, der bereits den Anlassfall zum Fall von Safe Harbor gab, wandte sich bzgl der Übermittlung seiner personenbezogenen Daten von Facebook Irland in die USA neuerlich an den EuGH. Das Recht und die Praxis der USA im Hinblick auf Datenzugriffe würden keinen ausreichenden Schutz vor dem Zugriff der Behörden bieten, so der Vorwurf. Zum einen wurden die „Standarddatenschutzklauseln" kritisiert (das sind Vertragsklauseln, die von der Kommission für den internationalen Datenverkehr erlassen werden), zum anderen wurde die Gültigkeit des Privacy Shields in Frage gestellt. Das Privacy Shield wurde eigentlich jährlich überprüft und für angemessen erklärt, nun wurde es aber in einem neuerlichen Verfahren vom EuGH für ungültig erklärt. Die Standardvertragsklauseln bleiben allerdings gültig.

Sind österreichische Unternehmen betroffen?

Ja. Jegliche Weiterleitung von personenbezogenen Daten in die USA ist grundsätzlich betroffen (zB viele Cloud-Lösungen, Office-Lösungen, Social Media Netzwerke, etc). Verwendet ein österreichisches Unternehmen zB Webtracking (zB „*Gefällt mir*"-Button bei Facebook), wickelt E-Mail-Accounts über die USA ab, nutzt Cloud-Lösungen mit Speicherung der Daten in den USA oder lagert schlichtweg diverse Datenverarbeitungsprozesse an Unternehmen mit Sitz in den USA aus, könnte das Unternehmen betroffen sein. Allerdings stützt sich nicht jeder Datenverkehr mit den USA auf das Privacy Shield.

Welche anderen Möglichkeiten für den internationalen Datenverkehr gibt es?

Angemessenheitsbeschlüsse sind nur eine Möglichkeit für einen rechtmäßigen internationalen Datenverkehr. Es gibt natürlich auch andere, wie zB das Vorliegen „geeigneter Garantien". Diese können zB in verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules), die von der zuständigen Aufsichtsbehörde genehmigt worden sind, bestehen oder in den oben bereits erwähnten Standarddatenschutzklauseln, die von der Europäischen Kommission erlassen oder von einer Aufsichtsbehörde angenommen und von der Kommission genehmigt worden sind. Auch eine ausdrückliche Einwilligung der betroffenen Personen im Einzelfall oder die Erforderlichkeit für die Erfüllung eines Vertrages mit der betroffenen Person kann eine Möglichkeit für den internationalen Datenverkehr sein (nähere Informationen dazu finden sich hier: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr).

Wo finde ich solche Standardvertragsklauseln?

Diese finden sich hier: Beschluss der Kommission vom 5. Februar 2010.

Wie geht es weiter? Was muss ein österreichisches Unternehmen tun?

Betroffenen Unternehmen sollten jetzt prüfen, welche Dienste sie in Anspruch nehmen und ob hier ein Datenaustausch mit den USA stattfindet. Wenn das bejaht wird, sollte geprüft werden, ob hierfür bisher das Privacy Shield herangezogen wurde. Wenn nicht, besteht derzeit noch kein Änderungsbedarf. Wenn ja, muss geklärt werden, ob eine andere Grundlage für den Datenverkehr herangezogen werden kann (alle weiteren Möglichkeiten finden sich hier: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr).

Große Konzerne und Diensteanbieter werden diese Prüfung voraussichtlich rasch durchführen und die erforderlichen Änderungen schnell umsetzen. Aber ja: Das neue Urteil bringt einigen Mehraufwand mit sich und natürlich auch Rechtsunsicherheit im internationalen Datenverkehr mit den USA.

Stand: 16.07.2020