

White Paper

Facebook-Fanpage

Datenschutz-orientierter Umgang mit
Facebook-Fanpages für Betreiber
- eine Handlungsempfehlung

Florian Padberg

ITUSO GMBH | FRAUNHOFERSTRASSE 9 | 85221 DACHAU | WWW.ITUSO.DE

Inhaltsverzeichnis

Hintergrund	2
Folgerungen für den Fanpage-Betreiber – ToDo's	3
Definition einer geeigneten Rechtsgrundlage.....	3
Bereitstellen von Informationspflichten gem. Artikel 13 und 14 DSGVO speziell für den Betrieb von Facebook-Fanpages.....	3
Erweiterung der Datenschutzerklärung.....	3
Anpassung / Neuanlage einer Verarbeitungstätigkeit.....	4
Beantwortung des Fragenkatalogs der Datenschutzkonferenz.....	4
Bereithalten des Meldeformulars für Betroffenen-Anfragen.....	4
Berücksichtigung des Restrisikos	4
Abschließende Bemerkung	4
Exkurs: Der Facebook-Like-Button	5
Anhang	6
Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person (Artikel 13 der EU-DSGVO) – Facebook-Fanpage (Muster).....	6
Informationspflicht bei der Erhebung von personenbezogenen Daten bei Dritten (Artikel 14 der EU-DSGVO) – Facebook-Fanpage (Muster).....	8
Ergänzende Datenschutzerklärung für Facebook-Fanpages (Muster).....	10
Verarbeitungstätigkeit „Facebook-Fanpage“ (Muster).....	12
Fragenkatalog der Datenschutzkonferenz.....	16

Hintergrund

Der EuGH hat mit Datum vom 05.06.2018 (EuGH, C - 210/16)¹ ein wegweisendes Urteil zur Datenschutz-Stellung und den Verantwortlichkeiten von Facebook-Fanpages gesprochen. Der EuGH legt in seinem Urteil zu Grunde, dass Facebook auf dem Endgerät des Besuchers einer Fanpage Cookies setzt, um damit die eigenen Dienste zu optimieren. Zudem soll damit dem Fanpage-Betreiber ermöglicht werden, bestimmte Statistiken zu erhalten (sog. Facebook Insights), wobei dies Funktion nicht deaktiviert werden kann.

Ferner geht der EuGH davon aus, dass der Fanpage-Betreiber durch von Facebook zur Verfügung gestellte Einstellungen und Filter Kriterien für seine Zielgruppen festlegen kann. Der Fanpage-Betreiber beeinflusst die Datenverarbeitung und Aussagekraft der Statistik damit durch die Festlegung von Kriterien selbst im Rahmen der vorgegebenen Möglichkeiten. **Dies macht ihn nach Ansicht des EuGH neben Facebook zum Datenschutz-rechtlich Verantwortlichen**, auch wenn „... diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein [können], dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen ist.“

Anfang September 2018 reagierte die **Datenschutzkonferenz**, ein Gremium der deutschen Datenschutzbehörden, mit einem Beschluss, in welchem sie die Ansicht teilt, dass die Fanpagebetreiber neben Facebook verantwortlich seien, entsprechend eine Vereinbarung nach Artikel 26 DSGVO erforderlich und das Betreiben einer Fanpage ohne entsprechende Vereinbarung rechtswidrig sei. Auf diese Verlautbarung der Datenschutzkonferenz reagierte Facebook wiederum mit dem sog. „Page Insights Controller Addendum“, welches zwischenzeitlich abrufbar ist (https://www.facebook.com/legal/terms/page_controller_addendum).

Mit dem Addendum ergänzt Facebook seine Nutzungsbedingungen dahingehend, dass Facebook Ireland und der Facebook-Fanpage-Betreiber **gemeinsam verantwortlich** im Sinne der DSGVO sind und legt die Verantwortlichkeiten in Bezug auf die Insights-Daten fest. Die primäre Verantwortung für die Datenverarbeitung von Insights-Daten übernimmt Facebook Ireland ebenso wie die sich daraus ergebenden datenschutzrechtlichen Pflichten, insbesondere die Information nach Artikel 13,14 DSGVO sowie der Informationspflicht aus Artikel 26 Abs. 2 DSGVO. **Der Fanpagebetreiber muss jedoch einige Pflichten übernehmen bzw. übernimmt diese mit Betreiben der Fanpage:**

- So müssen beispielsweise **Anfragen von Betroffenen** binnen sieben Kalendertagen an Facebook weitergeleitet werden – dafür steht ein Formular zur Verfügung.
- Der Fanpage-Betreiber muss zudem sicherstellen, dass er eine **Rechtsgrundlage** für die Datenverarbeitung hat, den Verantwortlichen für die Datenverarbeitung benennt und „jedwede sonstigen geltenden rechtlichen Pflichten“ erfüllt.
- Hinzuweisen ist zudem darauf, dass Facebook in der Vereinbarung nach Artikel 26 DSGVO nur Bezug auf Daten im Rahmen der Insights Bezug nimmt. **Andere Datenverarbeitungen** im Zusammenhang mit der Fanpage sind nicht erfasst und unterliegen der Verantwortung des Fanpage-Betreibers. Denkbar ist dabei beispielsweise die Beantwortung von Fragen im Rahmen von Postings oder der Nachrichtenfunktion oder die Verarbeitung von Daten im Rahmen von über die Fanpage durchgeführten Verlosungen.

UPDATE-Hinweis: Im Rahmen der Überarbeitung der „Facebook Business Tools Terms“ Mitte 2020 wurde auch das relevante Controller-Addendum aktualisiert (hier https://www.facebook.com/legal/controller_addendum zu finden, gültig ab 31. August 2020). Dieses spezifiziert nun noch ein wenig klarer, dass der Fanpage-Betreiber nur für die Verarbeitungen zusammen mit Facebook Ireland als „Gemeinsam Verantwortlicher“ agiert, nicht jedoch für die dahinter liegenden Verarbeitungen durch Facebook USA. Eine Entwarnung ist das aber nicht, denn die in diesem Whitepaper dargelegten Aufgaben für den Fanpage-Betreiber bleiben die gleichen.

Folgerungen für den Fanpage-Betreiber – ToDo's

Definition einer geeigneten Rechtsgrundlage

Da eine Einwilligung nach Artikel 6 Abs. 1 lit. a) DSGVO derzeit an der technischen Umsetzbarkeit scheitert, kommt hier vorzugsweise das berechnete Interesse nach Artikel 6 Abs. 1 lit. f) DSGVO in Betracht. Dieses könnte in einer optimierten Darstellung der Leistungen des Fanpage-Betreibers und zielgerichteter Kommunikation mit Kunden und Bewerbern zu sehen sein. Inwieweit die Datenschutzbehörden diesen Weg jedoch „mitgehen“, ist noch fraglich, insbesondere im Hinblick darauf, dass die DSK in ihrem Positionspapier aus April 2018 darauf hinwies, dass der Betroffene bei einer Datenverarbeitung, die auf das berechnete Interesse gestützt wird, ein Widerspruchsrecht hat und nach ihrer Ansicht nicht erkennbar sei, wie ein Facebook-Seitenbesucher, der über keinen eigenen Account verfügt, dieses ausüben soll.

Bereitstellen von Informationspflichten gem. Artikel 13 und 14 DSGVO speziell für den Betrieb von Facebook-Fanpages

Hierbei sollte dann die unter 1. genannte Rechtsgrundlage verwendet werden. Die Informationspflichten können als PDF-Template zum Download auf der Website des Betreibers bereitgestellt werden.

Vorbefüllte Vorlagen für diese beiden Informationspflichten finden sich im Anhang zu diesem Paper.

Erweiterung der Datenschutzerklärung

Entsprechend der über die Verarbeitung personenbezogener Daten über Facebook Insights hinaus ergibt sich, dass eine eigene Datenschutzerklärung für die Facebook-Fanpage vorhanden sein muss (**eine solche spezielle Datenschutzerklärung findet sich im Anhang dieses Papers**). Diese kann auf der Website des Fanpage-Betreibers integriert werden und sollte auf der Facebook-Fanpage verlinkt sein. Es ist aber stets zu beachten, dass nicht mehr als zwei Klicks nötig sein sollten/dürfen, um den Text der Erklärung aufgerufen zu haben.

Aus der Reihe **möglicher Umsetzungsvarianten der Einbindung empfiehlt die ituso GmbH aktuell die Folgende:**

Auf der Fanpage befindet sich im Bereich „Info“ inzwischen ein Unterpunkt „Datenrichtlinie“. Dort kann ein direkter Link zu der speziellen Datenschutzerklärung auf der Website des Fanpage-Betreibers hinterlegt werden (nicht abschließend geklärt ist allerdings, inwieweit die Anordnung als Unterpunkt des Bereichs „Info“ dem Grundsatz der Transparenz und leichten Zugänglichkeit genügt. Dennoch sollte hier unbedingt der entsprechende Link eingefügt werden!). Die spezielle Datenschutzerklärung für die Fanpage sollte dann als eigene Unterseite angelegt werden, auf die bspw. auch aus der Standard-Datenschutzerklärung heraus verlinkt werden kann.

Anpassung / Neuanlage einer Verarbeitungstätigkeit

Der Fanpage-Betreiber muss den Prozess der Fanpage in seinem Verzeichnis der Verarbeitungstätigkeiten entsprechend Artikel 30 DSGVO beschreiben. Hierbei sollte genau definiert werden, welche Datenkategorien, Personengruppen und Datenempfänger in die Verarbeitung involviert sind.

Ein Beispiel für eine solche Dokumentation einer Verarbeitungstätigkeit findet sich im Anhang dieses Papers.

Beantwortung des Fragenkatalogs der Datenschutzkonferenz

Im Rahmen der Stellungnahme der Datenschutzkonferenz vom 05. September 2018 wurde ein Fragenkatalog aufgelegt, der als Grundlage für eine Datenschutz-orientierte Dokumentation vom Betreiber-Unternehmen einer Facebook-Fanpage beantwortet werden sollte.

Der Fragenkatalog findet sich im Anhang dieses Papers.

Bereithalten des Meldeformulars für Betroffenen-Anfragen

Ziel ist es, solche Anfragen effizient und zeitnah an Facebook weiterreichen zu können. Das Formular findet sich hier: <https://www.facebook.com/help/contact/308592359910928>

Berücksichtigung des Restrisikos

Es ist festzustellen, dass eine Facebook-Fanpage derzeit nicht mit abschließender Rechtssicherheit betrieben werden kann. Das Risiko kann jedoch durch die vorgeschlagenen Maßnahmen reduziert werden.

Zwar vertreten die Datenschutzbehörden eine klare Meinung, doch letztlich ist dies „nur“ die Meinung der Behörde, die noch durch kein Urteil oder weitergehende gesetzliche Regelungen gestützt wird. In einem möglichen behördlichen Verfahren käme es zu einer inhaltlichen Auseinandersetzung zu der Thematik, die in einem Abhilfeverlangen enden könnte. Also beispielsweise mit der Aufforderung an Fanpage-Betreiber, die Fanpage rechtsicher zu gestalten oder aus dem Netz zu nehmen. Dass direkt ein Bußgeld verhängt würde, halten wir für unwahrscheinlich, es kann aber selbstverständlich nicht ausgeschlossen werden.

Abschließende Bemerkung

Die ituso GmbH nimmt durch diese Handlungsempfehlung keine Rechtsberatung vor, es handelt sich ausschließlich um einen fachlichen Vorschlag bzgl. des Datenschutz-seitigen Umgangs des Facebook-Fanpage-Betreibers mit der Facebook-Fanpage auf Basis des Zeitpunktes der Veröffentlichung dieser Handlungsempfehlung (Update Juli 2020).

Exkurs: Der Facebook-Like-Button

Facebook befindet sich generell unter einer detaillierten Überwachung durch die Datenschutzbehörden sowohl diesseits als auch jenseits des Atlantik. Daher war es auch nicht verwunderlich, dass der EuGH inzwischen nachgelegt hat, was die Rechtsprechung speziell zu diesem Plattformbetreiber angeht:

Mit Urteil vom 29. Juli 2019 hat das Gericht klargestellt, dass ein weiteres verbreitetes Facebook-Feature, der „Gefällt mir!“-Button, in den meisten Fällen nicht datenschutzkonform eingesetzt wird. Er darf nämlich nur mit expliziter Vorabinformation an den Nutzer aktiviert werden, denn sobald er aktiviert ist sendet er Nutzerdaten an Facebook – noch bevor (!) der Nutzer den Button selbst betätigt hat, sondern schon bei Aufruf der Seite, die den Button enthält. Wenn der Like-Button eingesetzt wird, ist der Seitenbetreiber grundsätzlich mitverantwortlich für die Einhaltung der Datenschutzverpflichtungen, zusammen mit Facebook als Gemeinsamer Verantwortlicher (so wie bei der Fanpage auch).

Abhilfe schafft hier aus heutiger Sicht nur ein Zweiklang von Maßnahmen:

- 1) Vor der Aktivierung der Funktionalität des Like-Buttons ist eine explizite Einwilligung des Nutzers einzuholen, die natürlich auch sauber zu dokumentieren ist
- 2) In den Datenschutzhinweisen der Website muss auf die Konsequenzen der Einwilligung und der dann folgenden Aktivierung der Button-Funktionalität – also auf die Übertragung von Daten an Facebook – hingewiesen werden.

Es ist davon auszugehen, dass Facebook auch weiterhin intensiv beobachtet werden wird, somit sollte sich jedes Unternehmen, das Leistungen dieser Plattform einsetzt, stets eigenverantwortlich zu möglichen Risiken, Rechtsprechungen und Lösungsmöglichkeiten informieren.

Anhang

Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person (Artikel 13 der EU-DSGVO) – Facebook-Fanpage (Muster)

Angaben zum Verantwortlichen	
Verantwortlicher gemäß Artikel 4 Abs. 7 EU-DSGVO	Beispiel GmbH Beispielstraße 1 12345 Beispielstadt
Vertreter gemäß Artikel 4 Abs. 17 EU-DSGVO	Geschäftsführer: Bernd Beispiel Telefon: +49 (0)1234 - 56789 Telefax: +49 (0)1234 - 56780 E-Mail: info@beispiel.de
Datenschutzbeauftragter	Detlef Datenschutz Beispiel GmbH Beispielstraße 1 12345 Beispielstadt E-Mail: datenschutz@beispiel.de

Zweck und Rechtsgrundlage	
Zweck der Verarbeitung	Unternehmens- und Leistungsdarstellung sowie Kommunikation mit Kunden & Interessenten mittels einer Facebook-Fanpage
Rechtsgrundlage	Berechtigtes Interesse des Verantwortlichen gem. Artikel 6 Abs. 1 lit. f) EU-DSGVO
Datenherkunft	Erhoben beim Betroffenen

Datenkategorien, betroffene Personengruppen, Empfänger, Ausland	
Datenkategorien	Personendaten, Kommentare, Bewertungen
Betroffene Personengruppen	Fanpage-Besucher
Empfänger	Intern: Marketing-Abteilung des Verantwortlichen Extern: Facebook (als gemeinsam Verantwortlicher)
Ausland	Eine Übertragung von personenbezogenen Daten in die USA findet im Rahmen des Betriebs der Facebook-Fanpage statt. Facebook ist dem EU-US-Privacy Shield beigetreten.

Zusätzliche Informationen	
Dauer der Speicherung	Die Speicherung Ihrer über die Facebook-Fanpage verarbeiteten personenbezogenen Daten erfolgt ausschließlich in den Systemen von Facebook und erlischt automatisch nach 2 Jahren.
Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit	Sie haben jederzeit das Recht Ihre Betroffenen-Rechte gegenüber den Verantwortlichen wahrzunehmen. Eine Anfrage an den Betreiber der Fanpage wird umgehend an Facebook zur Umsetzung weitergeleitet.
Recht auf Widerspruch	Sie können der Verarbeitung Ihrer personenbezogenen Daten über die Facebook-Fanpage jederzeit widersprechen. Bitte senden Sie dazu eine E-Mail an widerspruch@beispiel.de. Ihr Anliegen wird dann umgehend an Facebook weitergeleitet.
Beschwerderecht bei einer Aufsichtsbehörde	Sie haben das Recht jederzeit eine Beschwerde bei einer Aufsichtsbehörde einzureichen.
Mögliche Folgen des Widerspruchs.	Die Folge des Widerspruchs ist die Beantragung der Löschung Ihrer über die Facebook-Fanpage erhobenen personenbezogenen Daten bei Facebook.

Informationspflicht bei der Erhebung von personenbezogenen Daten bei Dritten
(Artikel 14 der EU-DSGVO) – Facebook-Fanpage (Muster)

Angaben zum Verantwortlichen	
Verantwortlicher gemäß Artikel 4 Abs. 7 EU-DSGVO	Beispiel GmbH Beispielstraße 1 12345 Beispielstadt
Vertreter gemäß Artikel 4 Abs. 17 EU-DSGVO	Geschäftsführer: Bernd Beispiel Telefon: +49 (0)1234 - 56789 Telefax: +49 (0)1234 - 56780 E-Mail: info@beispiel.de
Datenschutzbeauftragter	Detlef Datenschutz Beispiel GmbH Beispielstraße 1 12345 Beispielstadt E-Mail: datenschutz@beispiel.de

Zweck und Rechtsgrundlage	
Zweck der Verarbeitung	Unternehmens- und Leistungsdarstellung sowie Kommunikation mit Kunden & Interessenten mittels einer Facebook-Fanpage
Rechtsgrundlage	Berechtigtes Interesse des Verantwortlichen gem. Artikel 6 Abs. 1 lit. f) EU-DSGVO
Datenherkunft	Erhoben bei einem Dritten

Datenkategorien, betroffene Personengruppen, Empfänger, Ausland	
Datenkategorien	Personendaten
Betroffene Personengruppen	Fanpage-Besucher
Empfänger	Intern: Marketing-Abteilung des Verantwortlichen Extern: Facebook (als gemeinsam Verantwortlicher)
Ausland	Eine Übertragung von personenbezogenen Daten in die USA findet im Rahmen des Betriebs der Facebook-Fanpage statt. Facebook ist dem EU-US-Privacy Shield beigetreten.

Zusätzliche Informationen	
Dauer der Speicherung	Die Speicherung Ihrer über die Facebook-Fanpage verarbeiteten personenbezogenen Daten erfolgt ausschließlich in den Systemen von Facebook und erlischt automatisch nach 2 Jahren.
Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit	Sie haben jederzeit das Recht Ihre Betroffenen-Rechte gegenüber den Verantwortlichen wahrzunehmen. Eine Anfrage an den Betreiber der Fanpage wird umgehend an Facebook zur Umsetzung weitergeleitet.
Recht auf Widerspruch	Sie können der Verarbeitung Ihrer personenbezogenen Daten über die Facebook-Fanpage jederzeit widersprechen. Bitte senden Sie dazu eine E-Mail an widerspruch@beispiel.de. Ihr Anliegen wird dann umgehend an Facebook weitergeleitet.
Beschwerderecht bei einer Aufsichtsbehörde	Sie haben das Recht jederzeit eine Beschwerde bei einer Aufsichtsbehörde einzureichen.
Mögliche Folgen des Widerspruchs.	Die Folge des Widerspruchs ist die Beantragung der Löschung Ihrer über die Facebook-Fanpage erhobenen personenbezogenen Daten bei Facebook.

Ergänzende Datenschutzerklärung für Facebook-Fanpages (Muster)

Die folgende spezielle Datenschutzerklärung sollte von der Facebook-Fanpage aus direkt erreichbar auf der Betreiber-Website implementiert werden (enthaltene Links müssen aktiv sein, **rot markierte Textteile müssen angepasst werden):**

Facebook-Fanpage

*Gemeinsam verantwortlich für die Fanpage sind Facebook Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland; im Folgenden Facebook Ireland) sowie wir, die **FIRMA, ADRESSE, E-MAIL, TELEFON, FAX**, im Folgenden: **FIRMENKURZBEZEICHNUNG** oder wir).*

Auf der Fanpage werden aktuelle Informationen rund um unser Unternehmen eingestellt und können von den Nutzern kommentiert und/oder mit einem Like versehen werden. Auch können Nutzer sogenannte Besucherbeiträge auf unserer Seite posten. Die Kommentare, Likes und Beiträge sind öffentlich sichtbar und somit ist auch öffentlich erkennbar, von wem sie jeweils hinterlassen wurden. Nutzer können zudem Nachrichten an uns senden, welche jedoch nicht öffentlich sichtbar sind.

Über die sogenannten Insights haben wir die Möglichkeit, bestimmte statistische, anonymisierte Daten zum Nutzerverhalten abzurufen (<https://www.facebook.com/business/a/page/page-insights>). Dies sind beispielsweise die Gesamtanzahl von Seitenaufrufen, „Gefällt mir“-Angaben, Seitenaktivitäten, Beitragsinteraktionen, Reichweite, Videoansichten, Beitragsreichweite. Ebenfalls werden auf diesem Wege Daten zu den mit unserer Facebook-Seite verknüpften Facebook-Gruppen bereitgestellt.

Die Insights-Daten werden von Facebook mittels Cookies erzeugt und bereitgestellt. Wir können lediglich den Zeitraum, für welchen wir die Auswertung betrachten möchten, verändern. Außerdem können wir bestimmte Einstellungen für die Zielgruppe unserer Beiträge festlegen, welche sich entsprechend in der Statistik auswirken. Die Insights-Funktion kann von uns nicht abgestellt werden. Facebook nutzt die Daten insbesondere zu Werbezwecken (Erstellung personalisierter Werbung), Erstellung von Nutzerprofilen und Marktforschungszwecken. Sofern der Besucher der Fanpage ein Facebook-Nutzerkonto besitzt und mit diesem während des Seitenaufrufes eingeloggt ist, erfolgt die Speicherung der von den Cookies zur Verfügung gestellten Informationen, geräteübergreifend. Facebook gibt, ohne dass wir dies beeinflussen können, Daten weiter, unter anderem an die Facebook Inc., den US-amerikanischen Mutterkonzern der Facebook Ireland. Diese ist unter dem EU-US Privacy Shield zertifiziert und gilt damit als datenschutzkonform im Sinne der DSGVO. Einzelheiten zur Datenverarbeitung durch Facebook sind hier zu finden: <https://www.facebook.com/policy.php>

Wir nutzen die Insights-Daten ebenso wie die übrigen ersichtlichen Daten, um unser Angebot auf unserer Facebook-Seite zu optimieren und mit den Nutzern zu interagieren. So nutzen wir beispielsweise die Angaben zu Besuchszeiten für eine zeitlich optimierte Planung unserer Beiträge. Informationen über die Art der verwendeten Endgeräte helfen uns dabei, unsere Beiträge etc. so zu gestalten, dass sie auf allen Arten von Endgeräten optimal dargestellt werden. Auf Basis Facebook-Nutzungsbedingungen, denen jeder Benutzer im Rahmen der Einrichtung seines Facebook-Profiles zugestimmt hat, können wir die Abonnenten und Fans der Seite identifizieren und deren Profile sowie weitere geteilte Informationen von ihnen einsehen.

Rechtsgrundlage für die Datenverarbeitung ist das berechtigte Interesse nach Artikel 6 Abs. 1 lit. f) DSGVO. Die Messung des Besucherverhaltens dient der optimierten Darstellung und Ausrichtung unseres Onlineangebotes auf Facebook sowie einer effektiven Kommunikation mit Ihnen.

Die Datenverarbeitung erfolgt auf Basis einer Vereinbarung zwischen den gemeinsam Verantwortlichen nach Artikel 26 DSGVO; Facebook Ireland ist primär Verantwortlicher im Sinne der DSGVO (Artikel 26) in Bezug auf die Insights-Daten:

https://www.facebook.com/legal/terms/page_controller_addendum. (Ab 31.08.2020: Im Übrigen ist das Controller Addendum zu den Facebook Business Tools Terms zu beachten:

https://www.facebook.com/legal/controller_addendum)

Ihre Betroffenenrechte können Sie sowohl uns als auch Facebook Ireland gegenüber geltend machen. Weitere Datenschutzinformationen zu Facebook Ireland gemäß Artikel 13 DSGVO sind hier abrufbar:

<https://www.facebook.com/about/privacy>

Verarbeitungstätigkeit „Facebook-Fanpage“ (Muster)

Allgemeine Angaben der Verarbeitungstätigkeit

Max Mustermann GmbH

Bezeichnung der Verarbeitungstätigkeit: Facebook Fanpage

Beschreibung / Zweck der Verarbeitung: Das Unternehmen betreibt eine Facebook-Fanpage zur Darstellung der Dienstleistungen, Produkte und Unternehmens-Neuigkeiten. Außerdem dient die Fanpage einer zielgerichteten Kommunikation und einem Austausch mit Kunden, Interessenten und Bewerbern. Des Weiteren werden die Facebook Insights-Auswertungen genutzt um die Fanpage und die Dienstleistungen des Unternehmens zu verbessern.

Unternehmen	Max Mustermann GmbH GmbH Mustermann Straße 33 DE 99999 Teststadt Info@mustermann.de www.mustermann.de
Leiter Organisation	Max Mustermann
Datenschutzbeauftragter	Max Meuer michael.assistenz@test.de
Bestellung	Intern
Bestellt am	31.07.2018

Grundangaben der Verarbeitungstätigkeit

Permanente Verarbeitungstätigkeit: Permanent

Verarbeitungsstatus: Aktiv

Verantwortliche der Verarbeitungstätigkeit:

Unternehmen	Ansprechpartner
Max Mustermann GmbH GmbH Mustermann Straße 33 DE - 99999 Teststadt	Claudia Umsatz 089-1111111 claudia.umsatz@mustermann.de
Facebook Ireland Ltd. Grand Canal Square 4 IE - 2 Dublin	- - -

Grundlagen, Personen- und Datenkategorien der Verarbeitung

Grundlagen der Verarbeitung: Wahrung der berechtigten Interessen des Verantwortlichen

Betroffene Personengruppen: Fanpage-Besucher

Datenkategorien: Personendaten
Kommentare
Bewertungen

Herkunft: persönlich erhoben beim Betroffenen

Art	Löschfrist	Sperrfrist in Jahre
Facebook Insights-Daten	2 Jahre	2

Datenempfänger / Übermittlung in ein Drittland oder internationale Organisation

Interne Datenempfänger
(Abteilungen Ihres Unternehmens): Marketing

Eine Übermittlung von personenbezogenen Daten findet in folgende Staaten statt:

Land	Stelle	Einstufung	Garantien
Vereinigte Staaten	Facebook	Drittland	EU-US-Privacy-Shield

Schutzbedarfsfeststellung

Datenkategorie	Vertraulichkeit	Integrität	Verfügbarkeit
Personendaten	3	2	2
Kommentare	1	1	1
Bewertungen	1	1	1

Risikoklassifizierung

Geringer Schutzbedarf:

Datenkategorie	Eintrittswahrscheinlichkeit	Auswirkung	Risikostufe
Kommentare	1	1	2
Bewertungen	1	1	2

Hoher Schutzbedarf:

Datenkategorie	Eintrittswahrscheinlichkeit	Auswirkung	Risikostufe
Personendaten	2	2	4

Allgemeine technische und organisatorische Maßnahmen des Unternehmens

Organisationskontrolle:	<ul style="list-style-type: none"> - Schulung und Sensibilisierung der Mitarbeiter - Regelung von Verantwortlichkeiten - Verpflichtungen und Dienstanweisungen - Verfahrens-, Dokumentations- und Programmierrichtlinien - Funktionstrennung
Zugangskontrolle:	<ul style="list-style-type: none"> - Absicherung der Gebäude, Fenster und Türen - Sicherheitsglas - Bruch- und Öffnungsmelder - Videoüberwachungs-Anlagen - Alarmanlagen - Zutrittskontroll-Systeme mit Chipkarten-Leser - Passwortsicherheitsrichtlinien - Zwei-Faktor-Benutzeranmeldung - Firewalls - digitale Zertifikate - Schutz vor Schadsoftware - Bildschirmsperre - aktuelle Nutzerverwaltung
Datenträgerkontrolle:	<ul style="list-style-type: none"> - Verschlüsselung von Daten und Datensystemen - Verschlüsselung von Datenträgern - Kontrollierte Vernichtung von Datenträgern - Absicherung der Daten / Datenträger bei Versand
Speicherkontrolle:	<ul style="list-style-type: none"> - Kennwortrichtlinie - Nutzerprofile und Rollenkonzept entsprechend des Sicherheits- und Berechtigungskonzepts
Benutzerkontrolle:	<ul style="list-style-type: none"> - Kennwortrichtlinie - Nutzerstammdatensatz - Sperrung von Systemen - Kontrolle der Verbindungen
Zugriffskontrolle:	<ul style="list-style-type: none"> - Festlegung und Prüfung der Zugriffsberechtigungen - Protokollierung von Zugriffen - zeitliche Begrenzung von Zugriffen - revisionsfähige Dokumentation der Benutzerprofile
Übertragungskontrolle:	<ul style="list-style-type: none"> - Verschlüsselung und VPN für Zugriff von außen durch Mitarbeiter - CDs & Sticks mit geeigneten Schutzmechanismen (Verschlüsselung) - E-Mails mit Transportverschlüsselung - Ausgangs-Rechnungen mit digitaler Signatur - VPN-Tunnel
Eingabekontrolle:	<ul style="list-style-type: none"> - Standardmäßig Protokollierung von Inhaltlichen Änderungen und bei Änderungen in internen Systemen

Transportkontrolle:	<ul style="list-style-type: none">- Verschlüsselung von Datenträgern (USB, Festplatten, Bänder...)- Verschlüsselung von Datensystemen (Laptop, Mobiltelefon...)- Verschlüsselung von Übertragungsverbindungen (SSL, TSL...)
Wiederherstellbarkeit:	<ul style="list-style-type: none">- Regelmäßige Backup-Verfahren nach dem Backup-Konzept- Daten-Spiegelung in externe Systeme
Zuverlässigkeit:	<ul style="list-style-type: none">- Systemanalysen- Netzüberwachung- Überwachung der Lebensdauer von Datenträgern
Datenintegrität:	<ul style="list-style-type: none">- Prüfsummen- Zeitstempel- Signaturen- Protokolle
Auftragskontrolle:	<ul style="list-style-type: none">- Eindeutige vertragliche Regelung- Verträge mit Auftragsverarbeitern
Verfügbarkeitskontrolle:	<ul style="list-style-type: none">- Regelmäßige Backup-Verfahren nach dem Backup-Konzept- USV- RAID Systeme- Aktuelle Firewall-Lösung auf allen betriebenen Systemen (Server und Clients)- Aktueller Virenschutz auf allen betriebenen Systemen (Server und Clients)
Trennungsgebot:	<ul style="list-style-type: none">- Mandantenfähiges System

Stellungnahme Datenschutzbeauftragter

Verarbeitungstätigkeit wird freigegeben vom Datenschutzbeauftragten: Ja.

Fragenkatalog der Datenschutzkonferenz

Die folgenden Fragen sollte ein Betreiber einer Facebook-Fanpage beantworten und im Rahmen seiner Datenschutz-Dokumentation auf Anfrage nachweisen können:

1. In welcher Art und Weise wird zwischen Ihnen und anderen gemeinsam Verantwortlichen festgelegt, wer von Ihnen welche Verpflichtung gemäß der DSGVO erfüllt? (Artikel 26 Abs. 1 DSGVO)
2. Auf Grundlage welcher Vereinbarung haben Sie untereinander festgelegt, wer welchen Informationspflichten nach Artikel 13 und 14 DSGVO nachkommt?
3. Auf welche Weise werden die wesentlichen Aspekte dieser Vereinbarung den betroffenen Personen zur Verfügung gestellt?
4. Wie stellen Sie sicher, dass die Betroffenenrechte (Artikel 12 ff. DSGVO) erfüllt werden können, insbesondere die Rechte auf Löschung nach Artikel 17 DSGVO, auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO, auf Widerspruch nach Artikel 21 DSGVO und auf Auskunft nach Artikel 15 DSGVO?
5. Zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeiten Sie die personenbezogenen Daten der Besucherinnen und Besucher von Fanpages? Welche personenbezogenen Daten werden gespeichert? Inwieweit werden aufgrund der Besuche von Facebook-Fanpages Profile erstellt oder angereichert? Werden auch personenbezogene Daten von Nicht-Facebook-Mitgliedern zur Erstellung von Profilen verwendet? Welche Löschfristen sind vorgesehen?
6. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden beim Erstauftritt einer Fanpage auch bei Nicht-Mitgliedern Einträge im sogenannten Local Storage erzeugt?
7. Zu welchen Zwecken und auf welcher Rechtsgrundlage werden nach Aufruf einer Unterseite innerhalb des Fanpage-Angebots ein Session-Cookie und drei Cookies mit Lebenszeiten zwischen vier Monaten und zwei Jahren gespeichert?
8. Welche Maßnahmen haben Sie ergriffen, um Ihren Verpflichtungen aus Artikel 26 DSGVO als gemeinsam für die Verarbeitung Verantwortlicher gerecht zu werden und eine entsprechende Vereinbarung abzuschließen?

Der Herausgeber dieses White Papers ist die ituso GmbH. Für weitere Fragen oder Unterstützung bei der Umsetzung der Facebook Fanpage kontaktieren Sie uns bitte.

Ihr Ansprechpartner

Florian G. Padberg
E-Mail: florian.padberg@ituso.de
Tel. 08142 4205020

ituso GmbH

Fraunhoferstraße 9
85221 Dachau
www.ituso.de

Über den Autor Florian Padberg

Florian G. Padberg ist zertifizierter Datenschutzbeauftragter und -auditor (TÜV) und Project Management Professional (PMP®) sowie ein erfahrener Marketing- & Vertriebs-Consultant. Er ist Geschäftsführer der ituso GmbH und als Fachexperte für den Datenschutz tätig. Er übernimmt bei zahlreichen Unternehmen die Funktion des externen Datenschutzbeauftragten und berät bundesweit zu Datenschutz-relevanten Fragestellungen.

Er veröffentlicht regelmäßig Fachbeiträge, bildet Datenschutzbeauftragte aus und referiert zu aktuellen Themen im Bereich Datenschutz.

Wissen, worauf es beim Datenschutz ankommt

Unsere Berater für den Datenschutz, externe Datenschutzbeauftragte und Datenschutz-Auditoren unterstützen Unternehmen aller Branchen und Größen bei der Umsetzung des Datenschutzes.

UNSER TIPP: BERATERTAG IN IHREM UNTERNEHMEN

Buchen Sie einen Datenschutz-Profi, der einen Tag nur Ihnen gehört. Besonders wertvoll wenn:

- Sie wissen, dass Sie sich um Ihren Datenschutz kümmern müssen, aber nicht genau wie Sie das Thema angehen sollen
- Sie erfahren möchten was Sie konkret tun müssen
- Sie einen Experten brauchen (z. B. externer DSB), sich aber nicht gleich binden möchten

IHR NUTZEN

- ✓ Individuelle Beratung für Ihr Unternehmen
- ✓ Konkreter Maßnahmenplan für Ihr Unternehmen
- ✓ Datenschutz Basis-Schulung für Mitarbeiter

Weitere Informationen unter www.ituso.de/beratertag

Die Dokumente im Anhang wurden mit Vorlagen der Datenschutzmanagement-Software DSM-Online erstellt.



DSM-ONLINE
DATENSCHUTZMANAGEMENT

Webbasierte Software zum professionellen Aufbau und Organisation des Datenschutzes für kleine und mittelständische Unternehmen.

Einfach. Intuitiv. Kostengünstig.

www.dsm-online.eu