



**Bayerisches Landesamt für
Datenschutzaufsicht**
Promenade 18 | 91522 Ansbach
Telefon: 0981 180093 0
Fax: 0981 180093 800
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ihre Kontaktperson

Ihr Zeichen / Ihr Schreiben vom Unser Aktenzeichen

/

Ansbach, 22.12.2023

Aufsicht nach Art. 58 Datenschutz-Grundverordnung (DS-GVO)

App- Prüfung

Anlagen:

Informationsblatt

Sehr geehrte Damen und Herren,

wir, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), überwachen die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, d. h. primär in den privaten bayerischen Wirtschaftsunternehmen, bei den freiberuflich Tätigen, in Vereinen sowie in Verbänden.

Im Rahmen dieser Überwachungstätigkeit führen wir sogenannte fokussierte Prüfungen durch, d.h. anlasslose Prüfungen die einen bestimmten Schwerpunkt haben. Schwerpunkt dieser schriftlichen Prüfung sind die Prozesse und Datenverarbeitungen die in der App ohne eine Einwilligung stattfinden.

Wie wir bereits in unserem Tätigkeitsbericht 2022 berichtet haben, wollen wir die Einhaltung der datenschutzrechtlichen Anforderungen nicht nur auf Webseiten, sondern auch vermehrt bei Apps prüfen. Trotz der nun gesetzlich klar festgeschriebenen Einwilligungspflicht für Zugriffe auf Endeinrichtungen, also beispielsweise das Setzen von Cookies oder das Auslesen von Werbe-IDs und anderen Identifiern, erhalten wir weiterhin eine sehr hohe Anzahl an Beschwerden und Kontrollanregungen in diesem Bereich.

Neben der Frage, ob eine rechtswirksame Einwilligung eingeholt wurde, insbesondere ob eine Option keine Einwilligung zu Erteilen auf erster Ebene vorhanden ist, werden oftmals Prozesse initiiert noch bevor ein Consent-Banner erscheint. Leider erfolgen gerade bei Apps Auslesevorgänge, ohne dass der Nutzer mit einem Consent-Banner interagiert hat, das heißt meist direkt nach dem Laden der App bei der ersten Nutzung.

Im Rahmen unserer gesetzlichen Aufgaben kontrollieren wir deshalb mit dieser fokussierten Prüfung zufällig ausgewählte Appbetreiber gezielt hinsichtlich der Einhaltung der datenschutzrechtlichen Voraussetzungen.

Wir fordern Sie auf, im ersten Prüfschritt lediglich die unten dargestellten Fragen im Hinblick auf die App „xxx“ zu beantworten, weitergehende Ausführungen sind derzeit nicht Teil dieser fokussierten Prüfung. Im beiliegenden Informationsblatt können Sie zudem allgemeine Hintergründe zur Prüfung und zum Schwerpunkt „Einsatz von Drittdiensten in Apps“ erfahren.

Für den Eingang Ihrer Stellungnahme haben wir uns spätestens den 15.02.2024 vorgemerkt.

Sollten Sie dieser Aufforderung nicht fristgerecht nachkommen, stellen wir Ihnen den Erlass einer förmlichen Anweisung gem. Art. 58 Abs. 1 a) DS-GVO samt Zwangsgeldandrohung in Aussicht.

Im weiteren Prüfverlauf behalten wir es uns vor, Verantwortliche anlassbezogen vertiefter, ggf. mit einem breiteren Fokus und auch vor Ort zu kontrollieren, um uns von der erfolgreichen Umsetzung der datenschutzrechtlichen Vorgaben zu überzeugen. Ebenso können Dokumentationen und andere Unterlagen zu den abgefragten Themenschwerpunkten im weiteren Prüfverlauf angefordert werden.

Gesetzliche Informationen:

Die Datenschutz-Grundverordnung legt in Art. 58 Abs. 1 Buchst. a) fest, dass jede Aufsichtsbehörde über die Befugnis verfügt, den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich ist. Daneben verfügt jede Aufsichtsbehörde über die Befugnis, von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig ist, zu erhalten (vgl. Art. 58 Abs. 1 Buchst. e) DS-GVO). Ein Verstoß gegen diese Verpflichtung stellt eine Ordnungswidrigkeit dar und kann mit einer Geldbuße geahndet werden.

Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nrn. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde (§ 40 Abs. 4 Satz 2 Bundesdatenschutzgesetz). Die Inanspruchnahme des Auskunftsverweigerungsrechts ist mitzuteilen und nachvollziehbar zu begründen.

Mit freundlichen Grüßen

Dieses Anschreiben wurde maschinell versendet und ist daher ohne Unterschrift gültig.

Hinweise zur Verarbeitung Ihrer personenbezogenen Daten:

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten im Rahmen des vorliegenden Kontakts ist das Bayerische Landesamt für Datenschutzaufsicht. Weitere Informationen zur Verarbeitung Ihrer Daten, insbesondere zu den Ihnen zustehenden Rechten, können Sie unserer Homepage unter www.lida.bayern.de/Informationen entnehmen oder auf jedem anderen Wege unter den o.g. Kontaktdaten bei uns erfragen.

Prüffragen:

1. Allgemeines

Bitte geben Sie an, welche Version der o.g. App aktuell ist und auf welche Version sich Ihre Ausführungen beziehen. Führen Sie weiterhin kurz den Zweck und die Hauptfunktion(en) der App aus, dies ist für die Beurteilung dessen was ein Nutzer bei Nutzung der App wünscht bzw. erwarten kann und somit für das Bestehen der jeweiligen Rechtsgrundlage relevant.

2. Prozesse nach § 25 TTDSG

1. Werden Drittdienste wie beispielsweise Google, Facebook, Appsflyer etc. in der App eingesetzt bzw. zum Betrieb der App genutzt? Wenn ja, welche und zu welchem Zweck?
2. Welche Prozesse die § 25 TTDSG unterfallen, werden **ohne** Einholung einer Einwilligung initiiert? Das heißt, welche Speicher- oder Auslesevorgänge (Setzen von Cookies, Auslesen von Geräte-IDs etc.) erfolgen ohne Einwilligung (z.B. direkt bei Start der App)?
Führen Sie aus, weshalb Sie sich hier auf die Ausnahme des § 25 Abs. 2 TTDSG berufen.
3. Wie wird für einwilligungspflichtigen Prozesse eine Einwilligung eingeholt?

3. Verarbeitung von personenbezogenen Daten

1. Welche personenbezogenen Daten werden – ohne eine Einwilligung - durch die App verarbeitet und zu welchem Zweck?

Führen Sie hier nur die Verarbeitungstätigkeiten auf, die **nicht** auf die Rechtsgrundlage Art. 6 Abs. 1 lit. a) DS-GVO gestützt werden.
2. Sind die Datenschutzbestimmungen bereits im App-Store einsehbar (z. B. über die von Google bereitgestellte Funktion „Datenschutzerklärung für Entwickler“)?
3. Sind die Datenschutzbestimmungen bei erstmaliger App-Nutzung sofort einsehbar (z. B. Pop-Up oder Info-Frame)?
4. Sind die Datenschutzbestimmungen innerhalb der App leicht auffindbar und einsehbar?