Verbraucherzentrale
Hamburg

Facebook-Datenleck: Sammelklage läuft weiter – jetzt noch anmelden!

Im Jahr 2021 wurden massenhaft persönliche Daten von Nutzerinnen und Nutzern der Social-Media-Plattform Facebook veröffentlicht. Allein in Deutschland gibt es Millionen Geschädigte. Sie können sich einer Sammelklage anschließen und Schadensersatz fordern, auch wenn die Sache aktuell beim Europäischen Gerichtshof liegt.



© istock.com/Kenneth Cheung

DAS WICHTIGSTE IN KÜRZE

1. Im Jahr 2021 gab es ein umfassendes Datenleck bei Facebook, von dem 530 Millionen Konten betroffen waren.

2. Der Verbraucherzentrale Bundesverband (vzbv) erhob daraufhin eine Sammelklage gegen Meta. Gefordert werden 100 Euro bzw. zusätzliche Beträge von bis zu insgesamt 600 Euro, wenn weitere sensible Daten betroffen waren. Ein konkreter finanzieller Schaden ist nicht nachzuweisen.
3. Verhandelt wird vor dem Hanseatischen Oberlandesgericht. Eine durch das Gericht angeregte Einigung konnte nicht erzielt werden.
4. Zuletzt hat das Gericht das Verfahren ausgesetzt und mehrere Rechtsfragen dem Europäischen Gerichtshof (EuGH) zur Klärung vorgelegt.
5. Betroffene können sich weiterhin in das Klageregister eintragen. Dadurch bleiben mögliche Ansprüche gesichert.

Stand: 10.07.2026

Im Jahr 2021 wurden massenhaft persönliche Daten von Nutzerinnen und Nutzern der Social-Media-Plattform Facebook öffentlich im Internet gefunden. Allein in Deutschland gibt es Millionen Geschädigte. War Ihre Mail-Adresse auch dabei?

Dann können Sie sich der laufenden **Sammelklage des Verbraucherzentrale Bundesverbands (vzbv)** anschließen, um Schadensersatz zu erhalten. Im letzten Verhandlungstermin am 27. März 2026 regte das Hanseatische Oberlandesgericht in Hamburg einen **Vergleich** an. Nachdem eine Einigung im Rahmen der angeregten Vergleichsgespräche nicht zustande kam, hat das Hanseatische Oberlandesgericht mehrere Rechtsfragen dem Europäischen Gerichtshof zur Vorabentscheidung vorgelegt.

Vom Datenleck betroffen waren unter anderem Telefonnummern, Namen, E-Mail-Adressen, Geburtsdaten, Wohnorte und der Beziehungsstatus. Die Daten stammen von Nutzerprofilen aus den Jahren 2018 und 2019 und wurden von unbekannten Dritten mithilfe von bestimmten Programmiercodes systematisch gesammelt. Dieses Verfahren nennt sich „**Scraping**“ (dt. „Schürfen“) und steht für das automatisierte „Abschürfen“ öffentlich sichtbarer Daten aus Profilen, Foren und Webseiten, die dann an Dritte weiterverkauft werden.

Seitdem haben Kriminelle die Daten für unterschiedlichste Betrugs- und Täuschungsversuche missbraucht – etwa für Phishing-Mails, betrügerische

Kontaktaufnahmen oder Identitätsdiebstahl.

Sammelklage gegen Meta

Der Verbraucherzentrale Bundesverband (vzbv) hat gegen Meta Platforms Klage eingereicht. Verhandelt wird vor dem Hanseatischen Oberlandesgericht in Hamburg.

Wie ist der aktuelle Stand des Verfahrens?

Das Hanseatische Oberlandesgericht hat das Verfahren derzeit ausgesetzt und mehrere Fragen dem Europäischen Gerichtshof (EuGH) zur Entscheidung vorgelegt. Der EuGH soll insbesondere klären, welche verfahrensrechtlichen Voraussetzungen für die Musterfeststellungsklage gelten. Die Vorlage an den Europäischen Gerichtshof bedeutet keine Vorentscheidung über den Ausgang des Verfahrens. Sie dient dazu, zentrale Rechtsfragen zu klären, bevor das Verfahren in Hamburg fortgesetzt wird.

Bis zu einer Entscheidung des Gerichts in Luxemburg ruht das Verfahren. Trotz der Aussetzung können Sie sich als Betroffene oder Betroffener weiterhin in das Klageregister eintragen und so ihre möglichen Ansprüche sichern.

Was wird von Meta gefordert?

Ziel des Verfahrens ist die gerichtliche Feststellung, dass Meta für das Datenleck verantwortlich ist und betroffenen Nutzerinnen und Nutzern Schadensersatzansprüche zustehen.

- **100 Euro Grundbetrag**
- zusätzliche Beträge von bis zu insgesamt **600 Euro**, wenn weitere sensible Daten betroffen waren

Als Betroffene oder Betroffener müssen Sie **keinen konkreten finanziellen Schaden** nachweisen.

Wer kann sich der Sammelklage anschließen und wie?

Die Voraussetzungen für die Teilnahme an der Sammelklage sind daher überschaubar:

- **ein privates Facebook-Profil in den Jahren 2018 und/oder 2019**
- Angabe **einer Telefonnummer im Profil** (unerheblich ob öffentlich oder nicht öffentlich)

Nur wer im Klageregister eingetragen ist, wird offizieller Teil des Verfahrens – und damit auch des möglicherweise ausgehandelten Vergleichs. Der Eintrag schützt die eigenen Ansprüche vor der Verjährung – unabhängig davon, wie lange das Verfahren noch dauert. So gehen Sie vor:

- Erstens: Klage-Check machen (dort lässt sich auch überprüfen, ob man betroffen ist)
- Zweitens: Im Klageregister beim Bundesamt für Justiz eintragen

Mehr Infos: Die häufigsten Fragen zur Klage der Verbraucherzentrale wegen des Datenlecks bei Facebook werden auf verbraucherzentrale.de kompakt beantwortet.

Zweite Sammelklage gegen Meta

Neben dem Scraping-Fall steht Meta wegen eines weiteren Sachverhalts in der Kritik. Über unternehmenseigene Tracking-Tools, die auf zahlreichen externen Webseiten und Apps eingebunden sind, sollen umfangreiche Nutzungsdaten an Meta übermittelt worden sein – unter Umständen sogar selbst dann, wenn Nutzer und Nutzerinnen ausgeloggt waren oder die Tracking-Einstellungen angepasst hatten. Das Oberlandesgericht München entschied im Dezember (Urteil vom 18. Dezember 2025, Az. 14 U 1068/25 e), dass dieses Verhalten rechtswidrig sei und Betroffenen Schadensersatzansprüche zwischen 250 und 700 Euro zustehen können.

Der Verein zum Schutz von Verbraucherinteressen (Verbraucherschutzverein) aus Österreich hat in dieser Sache eine **Sammelklage** eingereicht. Auch Menschen aus Deutschland können sich daran beteiligen. Mehr erfahren Sie auf der Website des Verbraucherschutzvereins. Einen direkte Anmeldung ist auch über das Verbandsklageregister beim Bundesamt für Justiz möglich.

Allerdings sollten Sie Geduld mitbringen. Bis zur endgültigen Entscheidung können Jahre vergehen.

So schützen Sie Ihre persönlichen Daten

Die aktuellen Fälle zeigen einmal mehr, wie schnell Betroffene die Kontrolle über persönliche Daten verlieren können, wenn diese unbemerkt in Umlauf gelangen – und dass jede Person plötzlich Opfer von Betrug, Nachstellungen oder Identitätsmissbrauch werden.

Als Nutzerin oder Nutzer haben Sie grundsätzlich das Recht, alte Infos über sich von Seiten und Suchmaschinen entfernen zu lassen. Noch besser ist es aber, wenn persönliche Informationen gar nicht erst ins Internet gelangen. Hierzu empfehlen sich die folgenden Hinweise:

- **Nicht alles online stellen:** Was einmal im Internet steht, bleibt oft dauerhaft abrufbar. Fragen Sie sich vor jeder Veröffentlichung: „Würde ich diese Information Fremden mitteilen?“ Sensible Daten wie Geburtsdatum, Adresse oder Arbeitgeber sollten nur mit Bedacht geteilt werden. Auch vermeintlich private Fotos oder Posts können durch Sicherheitslücken, Apps oder Screenshots in falsche Hände geraten.
- **Eigene Daten regelmäßig googeln:** Überprüfen Sie gelegentlich, was online über Sie zu finden ist. Unliebsame Inhalte können Sie bei den Betreibern der Seiten löschen und bei Suchmaschinen entfernen lassen.
- **Alte Daten und Konten löschen:** Alte Profile, Forenbeiträge oder Apps, die Sie nicht mehr nutzen, sollten Sie löschen lassen. Wichtig: Die App zu löschen, bedeutet häufig nicht, dass das Konto gelöscht ist. Dieses muss aktiv gelöscht werden.
- **Starke Passwörter & Zwei-Faktor-Authentifizierung nutzen:** Jede Anmeldung sollte ein eigenes Passwort haben; Passwort-Manager können helfen. Zusätzlich empfehlen wir, eine Zwei-Faktor-Authentifizierung einzurichten, nicht das Login über Apple, Google oder Facebook (Single Sign-On) zu nutzen und Passwörter nicht mehrmals zu verwenden.
- **App-Berechtigungen prüfen:** Viele Apps wollen mehr Zugriff als nötig – besonders auf Kontakte (davon sind auch andere Menschen betroffen). Prüfen Sie vor der Installation neuer Apps genau, ob Sie Kamerazugriff, Standort, Mikrofon, Kontakte und den Zugriff auf Dateien gewähren sollen.
- **WLAN bzw. Standort unterwegs deaktivieren:** Aktiviertes WLAN oder GPS kann Geräte identifizierbar machen und Bewegungsprofile ermöglichen. Sind WLAN und

Standort deaktiviert, schont das außerdem die Akkuladung.

- **Cookies bewusst einstellen:** Cookies ermöglichen oft umfangreiche Nutzerprofile. Prüfen Sie daher Cookie-Banner auf Websites aufmerksam, erlauben Sie nur technisch notwendige Cookies und klicken Sie keinesfalls vorschnell auf „Alle Cookies akzeptieren“.
- **Weitere vorbeugende Hinweise und Tipps:** Wie kann ich mich vor einem Identitätsdiebstahl schützen?

ÜBRIGENS

Regelmäßig werden große Mengen an Daten, wie E-Mail-Adressen und Passwörter, gestohlen. Ob Ihre persönlichen Daten von Datenlecks betroffen sind, können Sie auf den folgenden Internetseiten der Universität Bonn (https://leakchecker.uni-bonn.de) oder des Hasso-Plattner-Instituts (https://sec.hpi.uni-potsdam.de/ilc/search?) durch Eingabe Ihrer E-Mail-Adresse prüfen lassen.

© Verbraucherzentrale Hamburg e. V.

https://www.vzhh.de/themen/telefon-internet/datenschutz/facebook-datenleck-sammelklage-laeuft-weiter-jetzt-noch-anmelden