4/2025
73 – 96

FAQ
Video an Polizei?
Viktoria Haidinger

# DATENSCHUTZ KONKRET

**Recht | Projekte | Lösungen**

Chefredaktion: Rainer Knyrim

## Marketing

### Der Sinn fürs Technische beim OGH
*Interview mit Georg Kodek, OGH*

### Voraussetzungen für einwilligungsloses Online-Tracking
*Michael Löffler, Jan Hospes*

### Checkliste E-Mail-Marketing
*Hans-Jürgen Pollirer*

### Informations-E-Mails
*Viktoria Haidinger*

### Neue Verbandsklage – verbessertes Private Enforcement
*Karl Wörle*

### Update zur Videoüberwachung
*Reinhard Hübelbauer*

### Löschung von Daten aus dem Taufregister
*Peter Krömer*

### EuGH: Bemessung von Geldbußen
*Lukas Moormann*

ISSN 2313-5409
dako.manz.at
MANZ

Michael Löffler/Jan Hospes
privacy awareness e.U./Research Institute – Digital Human Rights Center

# Voraussetzungen für einwilligungsloses Online-Tracking

**User Tracking; Besucherstromanalyse; Online-Marketing; Serverside-Tracking, Cookieless-Tracking.** Mittels Serverside-Tracking können Informationen über Webseitenbesuchende gewonnen werden, ohne Cookies oder sonstige Informationen auf ihren Endgeräten zu speichern. Der Beitrag zeigt auf, welche datenschutzrechtlichen Herausforderungen sich bei dieser Art der Besucherstromanalyse stellen und unter welchen Voraussetzungen auf das Einholen von Einwilligungen verzichtet werden kann.

Bei elektronischer Kommunikation schützt neben der DSGVO die **ePrivacy-RL** die Privatsphäre.[1] Diese enthält ua Regelungen zur Speicherung von Informationen/den Zugriff auf diese in Endgeräten (Computer, Laptops, Mobiltelefone etc).[2] Für die Anwendbarkeit der Regelungen soll es keine Rolle spielen, wer die Informationen zuvor dort abgespeichert hat.[3] In Österreich sind die Regelungen in **§ 165 Abs 3 TKG 2021** umgesetzt. Diese Bestimmung erfasst neben Betreibern öffentlicher Kommunikationsdienste auch *„Anbieter eines Dienstes der Informationsgesellschaft“,* worunter idR auch Webseiten zu verstehen sind.[4] Deshalb finden sich auf zahlreichen Webseiten sog „Cookie-Banner“, die auf das Speichern von Informationen hinweisen. **Cookies** sind Textdateien, die Webseitenbetreibende auf den Endgeräten von Besuchenden speichern und die bei erneutem Aufruf durch dasselbe Endgerät wieder abgerufen werden können, um Informationen über Webseitenbesuchende zu erlangen.[5] Art 5 Abs 3 ePrivacy-RL ist technologieneutral verfasst, daher wird das Speichern von Informationen generell erfasst (etwa auch in einer Datenbank des Webbrowsers).

Das Abspeichern/Auslesen von Informationen ist erst nach Erteilung einer Einwilligung zulässig.[6] Diese wird meist mittels **„Cookie-Bannern“** eingeholt. Eine Ausnahme besteht, wenn die Datenspeicherung/-ermittlung **unbedingt erforderlich** ist, um einen von Webseitenbesuchenden **ausdrücklich gewünschten** Dienst zur Verfügung zu stellen. Bei der Beurteilung, ob dies der Fall ist, muss auf die technische – nicht wirtschaftliche – Notwendigkeit abgestellt werden.[7]

Für die Nutzung von Online-Marketing-Cookies ist daher **idR eine Einwilligung erforderlich.** Bloß weil sich ein Dienst (ausschließlich) aus Werbeeinnahmen finanziert, bedeutet dies nicht, dass ein Nachverfolgen („Tracking“) von Webseitenbesuchenden zu Marketingzwecken technisch unbedingt erforderlich ist. Auch personalisierte Online-Werbung ist von Webseitenbesuchenden nicht ausdrücklich gewünscht.[8]

Da oftmals keine Einwilligung für Marketing- oder sonstige Tracking-Cookies erteilt wird, stellen sich viele Webseitenbetreibende die Frage, ob sie Informationen über Webseitenbesuchende auch ohne das Einholen von Einwilligungen auswerten dürfen, wenn keine Informationen auf den Endgeräten gespeichert oder von diesen ausgelesen werden. Technisch könnte dies mittels sog Serverside- bzw Cookieless-Tracking erfolgen.

## Was ist Serverside- bzw Cookieless-Tracking?

Beim Serverside- bzw Cookieless-Tracking wird auf das Speichern von Informationen auf den Geräten von Webseitenbesuchenden verzichtet. Stattdessen wird versucht, diese durch jene Informationen zu individualisieren (auszusondern), die von ihren Geräten **im Zuge der Datenübertragung mitgeschickt** werden oder die abgefragt werden können, ohne zuvor von Webseitenbetreibenden abgespeichert worden zu sein.[9] Oftmals ist es für Webseitenbetreibende nicht von Bedeutung, Personen namentlich zu identifizieren. Meist reicht es aus, Webseitenbesuchende voneinander zu unterscheiden. Erlauben es Informationen, Einzelpersonen auszusondern (englisch „singling out“), werden personenbezogene Daten verarbeitet und muss Datenschutzrecht eingehalten werden.[10]

Dabei kommen im Zuge der Datenübertragung neben IP-Adressen eine Vielzahl von Informationen infrage, etwa genutztes Betriebssystem, verwendete Sprache, Bildschirmauflösung, verwendeter Webbrowser und von diesen unterstützte Funktionen. Diese Informationen erlauben es in vielen Fällen, Webseitenbesuchende **auch ohne das Abspeichern** und Auslesen von Informationen auf Endgeräten zu **individualisieren.**[11] In der Praxis können Webseitenbesuchende idR bereits individualisiert werden, wenn (nur) ihre IP-Adresse[12] und Informationen über den von ihnen genutzten Webbrowser (sog User-Agent header)[13] verarbeitet werden.[14]

## Herausforderungen des TKG 2021 und der DSGVO

Die Lit ist sich uneinig, ob bereits das Nutzen von Informationen, die beim Aufruf von Webseiten von den Endgeräten der Webseitenbesuchenden mitgeschickt werden (und die nicht zuvor von Webseitenbetreibenden auf diesen gespeichert wurden), für nicht ausdrücklich von Webseitenbesuchenden gewünschte Zwecke, eine Einwilligung erfordert.[15]

UE muss die Frage, ob beim Serverside-Tracking eine Einwilligung erforderlich ist, aus **technischer Perspektive** beantwortet

[1] Zum Verhältnis von DSGVO und ePrivacy-RL s *Križanac* in *Knyrim*, DatKomm Art 95 DSGVO (Stand September 2024). [2] Art 5 Abs 3 ePrivacy-RL. [3] Vgl *Art. 29-Datenschutzgruppe*, Stellungnahme 9/2014 zur Anwendung der RL 2002/58/EG auf die Nutzung des virtuellen Fingerabdrucks (WP 224), 25. 11. 2014, 9. [4] Vgl *Forgó* in *Steinmaurer* (Hrsg), Telekommunikationsgesetz 2021 TKG 2021 (2025) § 165 Rz 9; *Zankl*, ECG (2016) Rz 48ff. [5] EuGH 1. 10. 2019, C-673/17, *Planet49*, Rn 31. [6] Die Einwilligung muss datenschutzrechtlichen Anforderungen genügen; DSB 19. 9. 2023, 2023–0.632.875. [7] Vgl VwGH 31. 10. 2023, Ro 2020/04/0024; BVwG 31. 7. 2024, W108 2280724-1; sa *Thiele*, BVwG: Google® reCAPTCHA ohne Einwilligung datenschutzwidrig, jusIT 2025/71. [8] Vgl BVwG 12. 3. 2019, W214 2223400-1; VwGH 31. 10. 2023, Ro 2020/04/0024. [9] S *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg*, FAQ zu Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, 03.2022, 16. [10] EuGH 7. 3. 2024, C-604/22, IAB Europ; BVwG 13. 9. 2024, W298 2274626-1; *Haidinger/Löffler*, Identifizierbarkeit durch Herausgreifen für Personenbezug ausreichend, Dako 2019/50). [11] Vgl *Löffler*, Datenschutzrechtliche Herausforderungen beim Besuchertracking, Dako 2022/15. [12] Zum Personenbezug von IP-Adressen s EuGH 19. 10. 2016, C-582/14, *Breyer*; bzw EuG 8. 1. 2025, T-354/22, *Bindl/Kommission*. [13] S *Mozilla*, User-Agent header; https://developer.mozilla.org/de/docs/Web/HTTP/Reference/Headers/User-Agent (Stand 21. 7. 2025). [14] Vgl *Art. 29-Datenschutzgruppe*, Stellungnahme 9/201, 6. [15] *Schürmann/Guttmann*, § 25 TTDSG – Anwendungsbereich und Ausnahmen, KuR 2023, 246.

werden. Abgestellt werden muss **erstens** auf die unbedingte Erforderlichkeit, Daten für die Erbringung ausdrücklich gewünschter Dienste zu verarbeiten. Werden zusätzliche Informationen verarbeitet (etwa durch das Einbinden von Scripten, die aktiv die Übermittlung darüber hinausgehender Informationen anfordern), braucht es hierfür idR eine Einwilligung.[16]

Beim Abruf von Webseiten befinden sich insb in den Log-Dateien von Webservern regelmäßig Informationen zur IP-Adresse von Webseitenbesuchenden, dem Zeitpunkt ihres Besuchs, Informationen zum genutzten Browser und darüber, ob die gewünschte Webseite fehlerfrei ausgeliefert wurde. Die Verarbeitung dieser Informationen könnte zu einer Anwendung von Art 5 Abs 3 ePrivacyRL führen.[17] Obwohl das Speichern dieser Log-Dateien technisch unterbunden werden könnte, sind sie sowohl aus datenschutzrechtlicher Perspektive als auch aus Sicht der Informationssicherheit betrachtet „unbedingt erforderlich", um einen fehlerfreien und sicheren Abruf der ausdrücklich gewünschten Webseite sicherzustellen.[18] Informationen aus Log-Dateien können technisch oft zur Individualisierung von Webseitenbesuchenden herangezogen werden, datenschutzrechtlich soll dies aber nicht ohne weiteres zulässig sein.[19]

Daher muss uE **zweitens** auf den **Zeitpunkt** abgestellt werden, ab dem Informationen aus Log-Dateien für nicht ausdrücklich von Webseitenbesuchenden gewünschte Zwecke (etwa Besucherstromanalysen) verwendet werden und auf die **Art**, wie dies erfolgt. Wurde eine Webseite fehlerfrei ausgeliefert, werden personenbezogene Daten in Log-Dateien idR nicht mehr benötigt.

Weder Art 5 Abs 3 ePrivacyRL noch § 165 Abs 3 TKG 2021 enthalten ausdrückliche Regelungen zur Verarbeitung von Daten, die zulässigerweise ohne Einwilligung ermittelt wurden, zu anderen Zwecken. Einigen Stellungnahmen in der Lit zufolge unterliegt die im Anschluss an einen Zugriff/eine Ermittlung erfolgende Datenverarbeitung den Regeln der DSGVO.[20] Diese verpflichtet grds zur unverzüglichen Löschung nicht mehr benötigter personenbezogener Daten.[21] Andere als personenbezogene Daten müssen nach der DSGVO nicht gelöscht werden. Daher stellt das Anonymisieren[22] ursprünglich personenbezogener Daten, ein Löschen personenbezogener Daten dar. Dies spricht für die Zulässigkeit von passivem Serverside-Tracking mittels anonymer Daten.[23] Im Anwendungsbereich der ePrivacyRL muss beachtet werden, dass sie nicht nur natürliche, sondern auch juristische Personen schützt.[24]

Die ehemalige ***Art. 29-Datenschutzgruppe*** stand der Verarbeitung digitaler Fingerabdrücke für sekundäre Zwecke kritisch gegenüber. Ihrer Ansicht nach muss für jeden Zweck gesondert beurteilt werden, ob nach den Regeln der ePrivacyRL eine Einwilligung eingeholt werden muss.[25] Als einwilligungspflichtig erachtete sie die Nutzung von digitalen Fingerabdrücken etwa für die Erstellung von Statistiken – selbst dann, wenn personenbezogene Daten hierfür anonymisiert würden.[26] Die von der Art. 29-Datenschutzgruppe betrachteten Situationen unterscheiden sich uE aber von jener, in der zulässigerweise ohne Einwilligung verarbeitete Daten nach dem Löschen personenbezogener Daten für einen anderen Zweck verarbeitet werden.

Sodann stellt sich noch die Frage, ob die Verarbeitung **anonymer Daten** zu nicht ausdrücklich gewünschten Zwecken bereits bei Ermittlung der für die Übertragung von Webseiten unbedingt erforderlichen Daten mitberücksichtigt werden muss. UE ist diese Frage mit Nein zu beantworten. Denn selbst wenn personenbezogene Daten zulässigerweise ermittelt wurden, müssen sie gelöscht werden, sobald sie für den designierten Zweck nicht mehr benötigt werden. Das Löschen ist somit die abschließende Handlung der Verarbeitung von Daten für einen bestimmten ausdrücklich gewünschten Zweck und in diesem Fall nicht als davon losgelöst zu erachtender Zweck.

Diese Überlegungen sprechen uE für die Zulässigkeit von Serverside-Tracking ohne Einwilligung. Bis zum Vorliegen höchstgerichtlicher Rsp muss allerdings auf das Restrisiko verwiesen werden, dass Behörden eine Einwilligung für die Weiterverarbeitung von Informationen aus Log-Dateien zur anonymen Besucherstromanalyse verlangen.

## Fazit

Mit § 165 Abs 3 TKG 2021 gelten strenge Regeln, wann personenbezogene Daten von Webseitenbesuchenden ermittelt werden dürfen. Webseitenbetreibende, welche den mit der Anonymisierung einhergehenden Informationsverlust in Kauf nehmen können (etwa, weil es ihnen nur auf Informationen über Besucherströme und nicht über individualisierte Besuchende ankommt), brauchen uE unter folgenden Bedingungen keine Einwilligung einzuholen.[27]

- Es werden nur Informationen verarbeitet, die von Webseitenbesuchenden übermittelt wurden und unbedingt erforderlich waren, um eine ausdrücklich von diesen gewünschte Webseite an sie zu übertragen (insb aus Log-Dateien), und
- diese Daten werden erst für andere Zwecke verarbeitet, nachdem sie anonymisiert wurden (dabei sind auch identifizierende Informationen juristischer Personen zu anonymisieren).[28]

Dako 2025/32

[16] Vgl *EDSA*, Leitlinien 2/2023 zum technischen Anwendungsbereich von Art 5 Abs 3 der Datenschutzrichtlinie für elektronische Kommunikation V2.0, 7. 10. 2024 Rn 33; *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste) V1.2, 11.2024, Rn 24. [17] *EDSA*, Leitlinien 2/2023, Rn 42f. [18] *Kastelitz/Gamper*, Verarbeitung von Protokolldaten: datenschutzrechtliches „Must-have", „Nice-to-have" oder „No-Go"? jusIT 2022/60. [19] *Art. 29 Datenschutzgruppe*, Stellungnahme 9/2014, 11f. [20] *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste) V1.2, 11.2024 Rz 25; *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. 12. 2021 V1.1, 12.2022 Rz 95f. Vgl *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg*, FAQ zu Cookies und Tracking 14. Zum Verhältnis von ePrivacyRL und DSGVO *EDSA*, Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO 12. 03. 2019, Rn 29. [21] Art 17 Abs 1 lit a DSGVO vgl auch *EDSA*, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen V2.0, 20. 10. 2020, Rn 75. [22] Bei der Beurteilung, ob Daten anonym sind, ist auf die (Re-)Identifizierungswahrscheinlichkeit abzustellen; *Riechert* in *Riechert/Wilmer* (Hrsg), TTDSG (2022) § 25 Rz 43. Anschaulich *Haidinger*, Der Weg von personenbezogenen zu anonymen Daten, Dako 2015/34; sa das beim EuGH anhängige Verfahren zur Klärung, ob es eine anonymisierende Wirkung der Pseudonymisierung gibt C-413/23 P. [23] So auch die CNIL in ihrem Selbstbewertungstool zur Zulässigkeit der Besucherzählung: www.cnil.fr/sites/default/files/2025-07/outil_d_auto-evaluation_mesure_d_audience.pdf. [24] *EDSA*, Leitlinien 2/2023, Rn 29 uVa ErwGr 26 ePrivacyRL. [25] *Art. 29-Datenschutzgruppe*, Stellungnahme 9/2014, 11f. [26] *Art. 29-Datenschutzgruppe*, Stellungnahme 9/2014, 10. [27] So im Ergebnis auch *Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg*, FAQ zu Cookies und Tracking 14ff. [28] *EDSA*, Leitlinien 2/2023, Rn 29 uVa ErwGr 26 ePrivacyRL.

## Zum Thema

### Über die Autoren

DI Michael Löffler ist Datenschutzexperte bei privacy awareness e.U.
E-Mail: michael.loeffler@privacyawareness.at
Mag. iur. Jan Hospes ist Senior Researcher und Senior Consultant am Research Institute – Digital Human Rights Center.
E-Mail: jan.hospes@researchinstitute.at

### Hinweis

Für eine konkrete Implementation des Serverside-Trackings siehe etwa die Informationen von JENTIS in *Knyrim/Ebner,* Katalysator für sensible Daten, Dako 2022/14.

Karl Wörle
Fachhochschule BFI Wien.

# Die neue Verbandsklage – verbessertes Private Enforcement im Datenschutzrecht

**Verbandsklage; Schadenersatz; Unterlassungsklage; Vergleich.** Mit der Verbandsklagen-RL wurde in Österreich eine zivilprozessuale „Gruppenklage", ähnlich der US class action eingeführt. Mit ihr verfügen Verbraucherschutzorganisationen über ein neues Instrument, gegen Datenschutzverstöße vorzugehen. Dieser Beitrag untersucht die Schnittstelle von Datenschutz- und Zivilprozessrecht mit Fokus auf Unterlassungsklagen, Verbandsklagen auf Abhilfe sowie die Bereinigung datenschutzrechtlicher Streitigkeiten durch Prozessvergleich.

### Einleitung

Die Verbandsklagen-RL[1] (VK-RL) ist in Österreich gut eineinhalb Jahre verspätet (infolge politischen Gegenwinds) mit Wirkung ab 18. 7. 2024 umgesetzt worden. Grundsätzlich als **Instrument des Verbraucherschutzes** konzipiert, soll sie wegen fortschreitender Digitalisierung auch im Datenschutz zur Anwendung kommen. Auch wenn die DSGVO seit jeher ein Nebeneinander verwaltungsbehördlicher und gerichtlicher Rechtsdurchsetzung (Art 77 ff) vorsieht, ist die österr Rechtslage internationalen Rechtsentwicklungen in diesem Bereich bislang hinterhergehinkt. Hier sei insb auf die großen data privacy litigations aus den USA verwiesen, wo etwa *Meta* im Cambridge-Analytica-Datenskandal 725 Millionen US-Dollar an Schadenersatz bezahlen musste.

Mit Umsetzung der VK-RL schließt sich Österreich internationalen Trends beim **datenschutzrechtlichen Private Enforcement** an. Die neue Rechtslage findet bereits Widerhall in der Praxis: So hat das von *Max Schrems* mitgegründete Europäische Zentrum für digitale Rechte (noyb) bekanntgegeben, bereits Klagen vorbereitet zu haben und 2025 einreichen zu wollen.[2]

### Die neue Verbandsklage im Überblick

In Österreich standen im kollektiven Rechtsschutz bislang zwei prozessuale Instrumente im Vordergrund: einerseits **Verbandsklagen auf Unterlassung** (gem der Unterlassungsklagen-RL[3]) und andererseits die Behelfslösung der **Sammelklage österreichischer Prägung**, bei der Verbraucher ihre Ansprüche an einen Sammelkläger abtreten. Dennoch klafften Rechtsschutzlücken.[4]

Auch in anderen EU-MS sind kollektive, prozessuale Werkzeuge eingerichtet, die jedoch weit hinter einem klägerfreundlichen Mechanismus wie der US class action zurückblieben. In diesem Flickwerk nationaler Kollektivverfahren führt die VK-RL einen neuen Mechanismus ein, der eine **kollektive Abhilfeklage** vorsieht, welche Leistungsklagen im engeren Sinn (insb auf Schadenersatz) ermöglicht.

Bei der Implementierung (Verbandsklagen-RL-Umsetzungs-Novelle, VRUN)[5] hat der österr Gesetzgeber die verfahrensrechtlichen Bestimmungen in die Zivilprozessordnung aufgenommen **(§§ 619–635 ZPO)**, während die rechtliche Stellung der klagebefugten Verbände (Qualifizierte Einrichtungen, QE) in einem eigenen Gesetz **(Qualifizierte-Einrichtungen-Gesetz, QEG)** geregelt werden.

**Als QE sind in Österreich insb der Verein für Konsumenteninformation, der Verbraucherschutzverein und noyb relevant.**

Es sei noch erwähnt, dass die VK-RL einen „Bestandschutz" für die national bereits eingerichteten Verfahren des kollektiven Rechtsschutzes vorsieht (Art 1 Abs 2). Unterlassungsverbandsklagen nach §§ 28 f KSchG sowie die Sammelklage österreichischer Prägung stehen also nach wie vor zur Verfügung.

### Anwendungsbereich

Der Datenschutz ist ein praxisrelevanter Anwendungsfall für **kollektives Private Enforcement**. Zumeist sind nämlich die In-

[1] VerbandsklagenRL 2020/1828 ABl L 2020/409. [2] https://noyb.eu/en/noyb-now-qualified-bring-collective-redress-actions (Stand aller Links 3. 4. 2025). [3] RL (EU) 2009/22/EG über Unterlassungsklagen zum Schutz der Verbraucherinteressen. [4] *Klauser/Kunz,* Mechanismen zur Durchsetzung kollektiver Verbraucherinteressen in Österreich, in *Anzenberger/Klauser/Nunner-Krautgasser (Hrsg)*, Kollektiver Rechtsschutz im Europäischen Rechtsraum (2022) 3 (6 f). [5] BGBl I 2024/85.