Rechtliche Gestaltung von E-Mail-Tracking & -Profiling

30. DFN-Konferenz „Sicherheit in vernetzten Systemen“
Hamburg, 09.02.2023

Christian Blaicher, Friederike Schellhas-Mende

secorvo
security consulting

Wer sind wir?

Christian Blaicher

Volljurist

Friederike Schellhas-Mende

Volljuristin

secorvo
security consulting

Secorvo Security Consulting

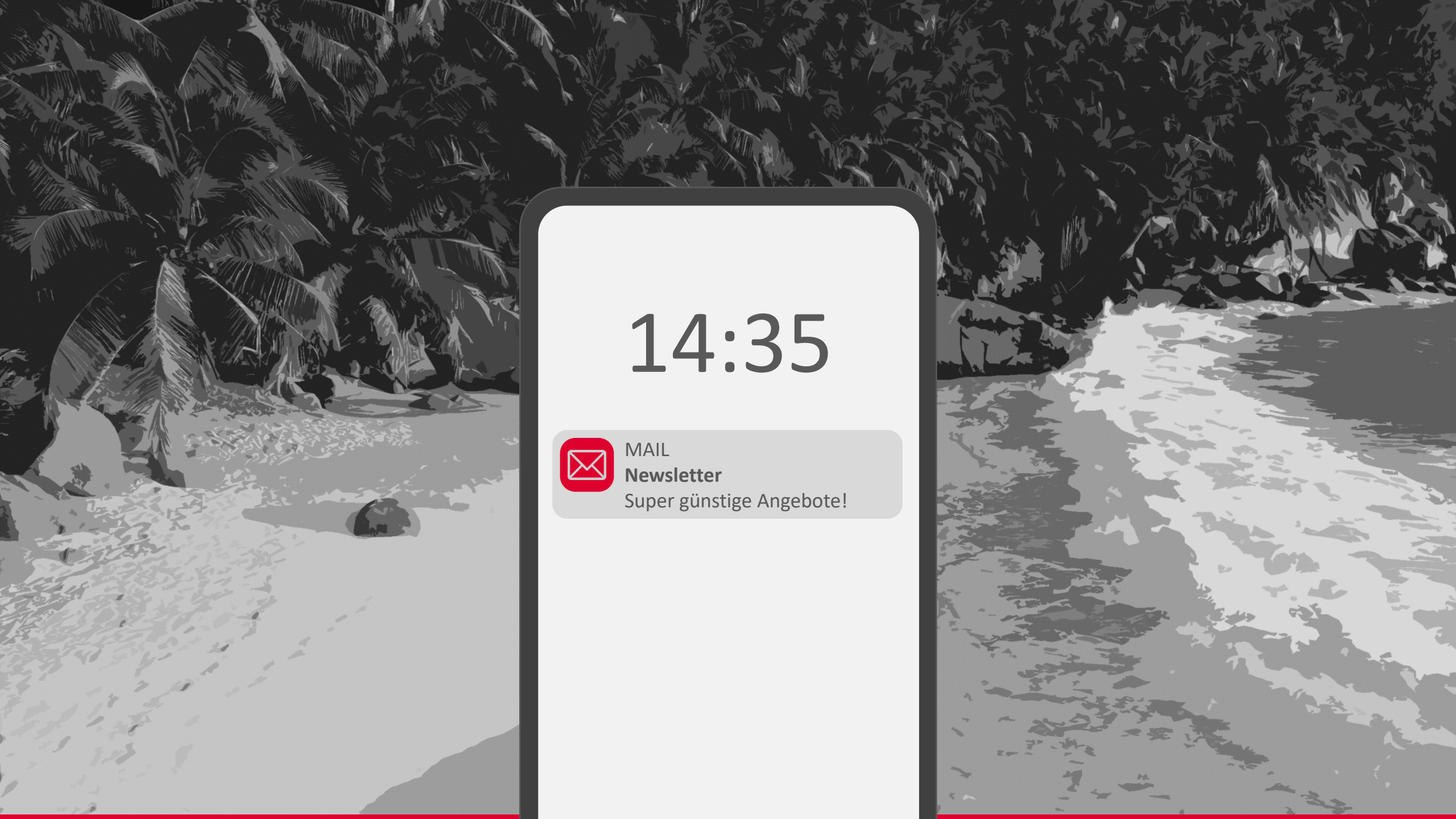
Tätigkeitsbereich

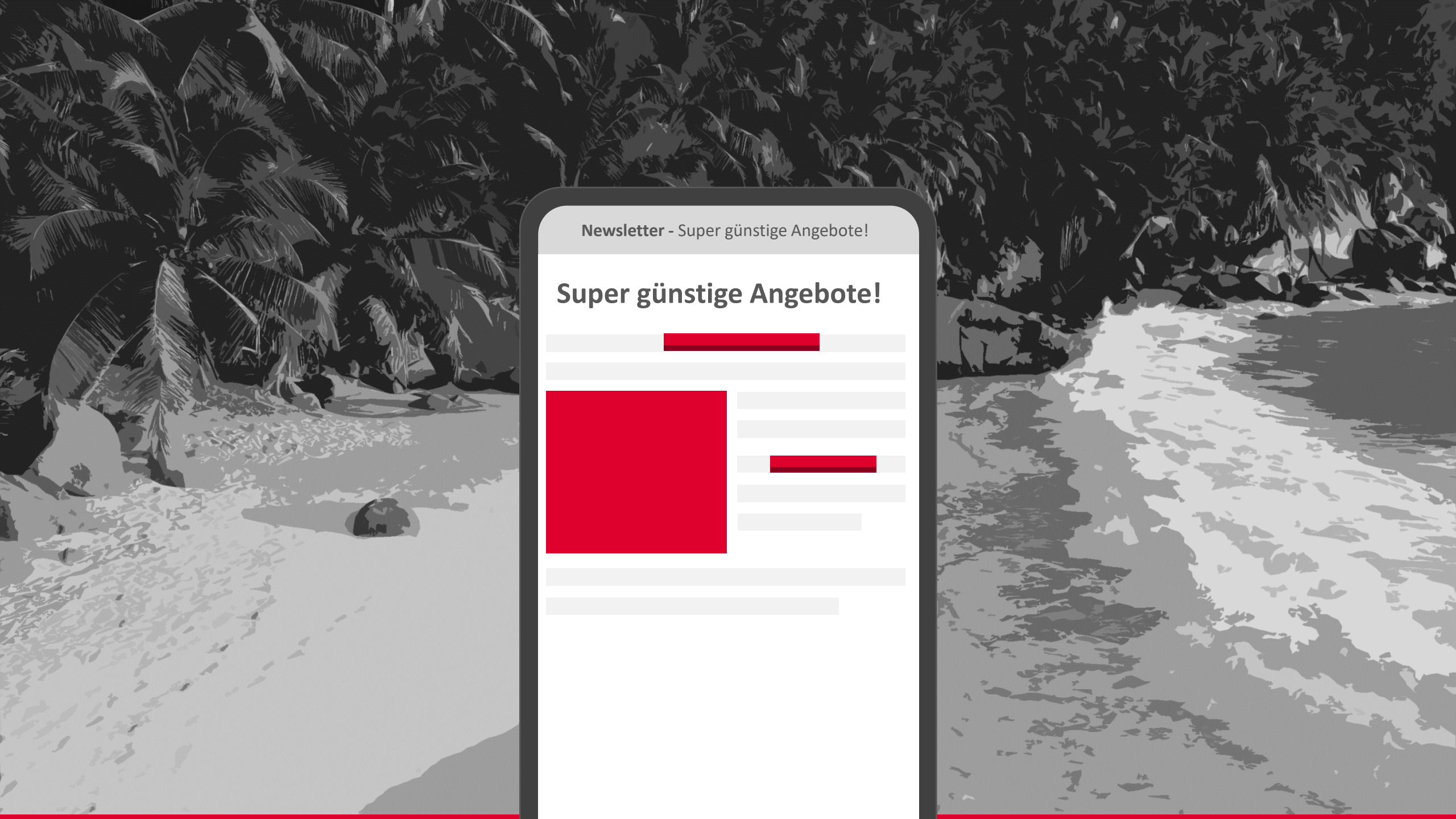
- Datenschutzberatung
  - Audit
  - Folgenabschätzung
  - Datenschutzbeauftragter
  - Coaching
  - Löschkonzept
- Forensische Analysen
- ISMS (ISO 27001) und IT-Grundschutz
- PKI
- Security Awareness
- Sichere Software

Seminare

- BSI Vorfall-Experte – Aufbauschulung
- IT-Sicherheit
  praxisnah und aktuell
- PKI
  Grundlagen, Vertiefung, Realisierung
- T.I.S.P.
  TeleTrusT Information Security Professional
- T.P.S.S.E.
  TeleTrusT Professional for Secure Software Engineering

secorvo
security consulting


14:35
MAIL
Newsletter
Super günstige Angebote!


Newsletter - Super günstige Angebote!
Super günstige Angebote!

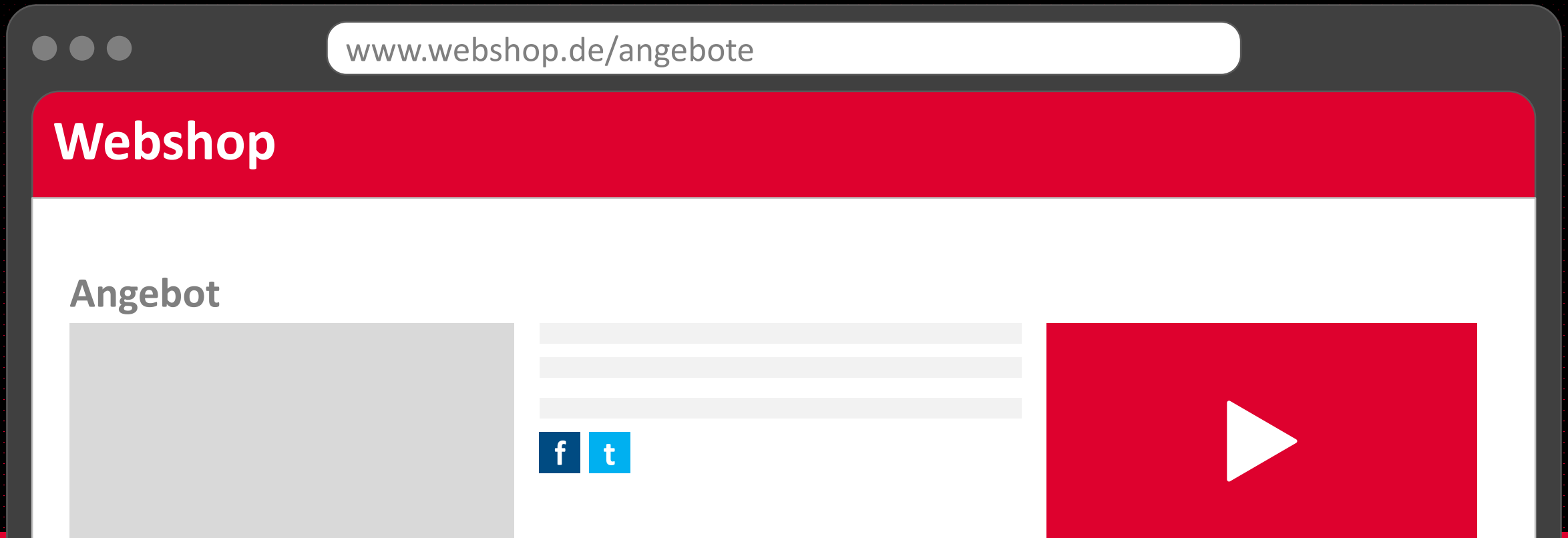
Der Absender erfährt, dass Sie…

- die E-Mail um 14:35 Uhr geöffnet haben
- die IP-Adresse 102.51.96.116 haben
- die Mail auf den Seychellen gelesen haben
- die Mail vermutlich zwei Minuten lang angesehen haben
- auf zwei Links geklickt haben

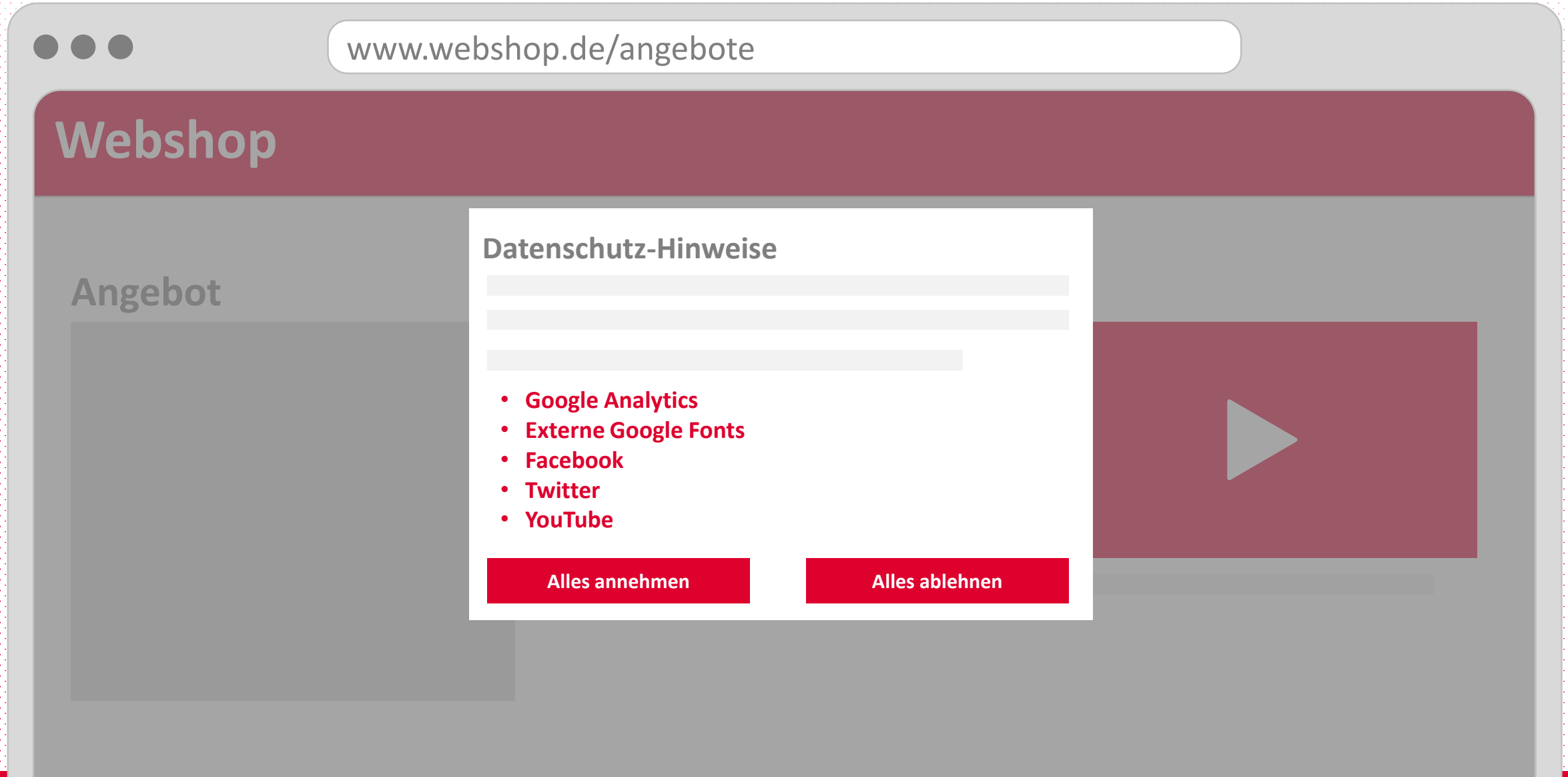
Warum dieser Vortrag?

Tracking

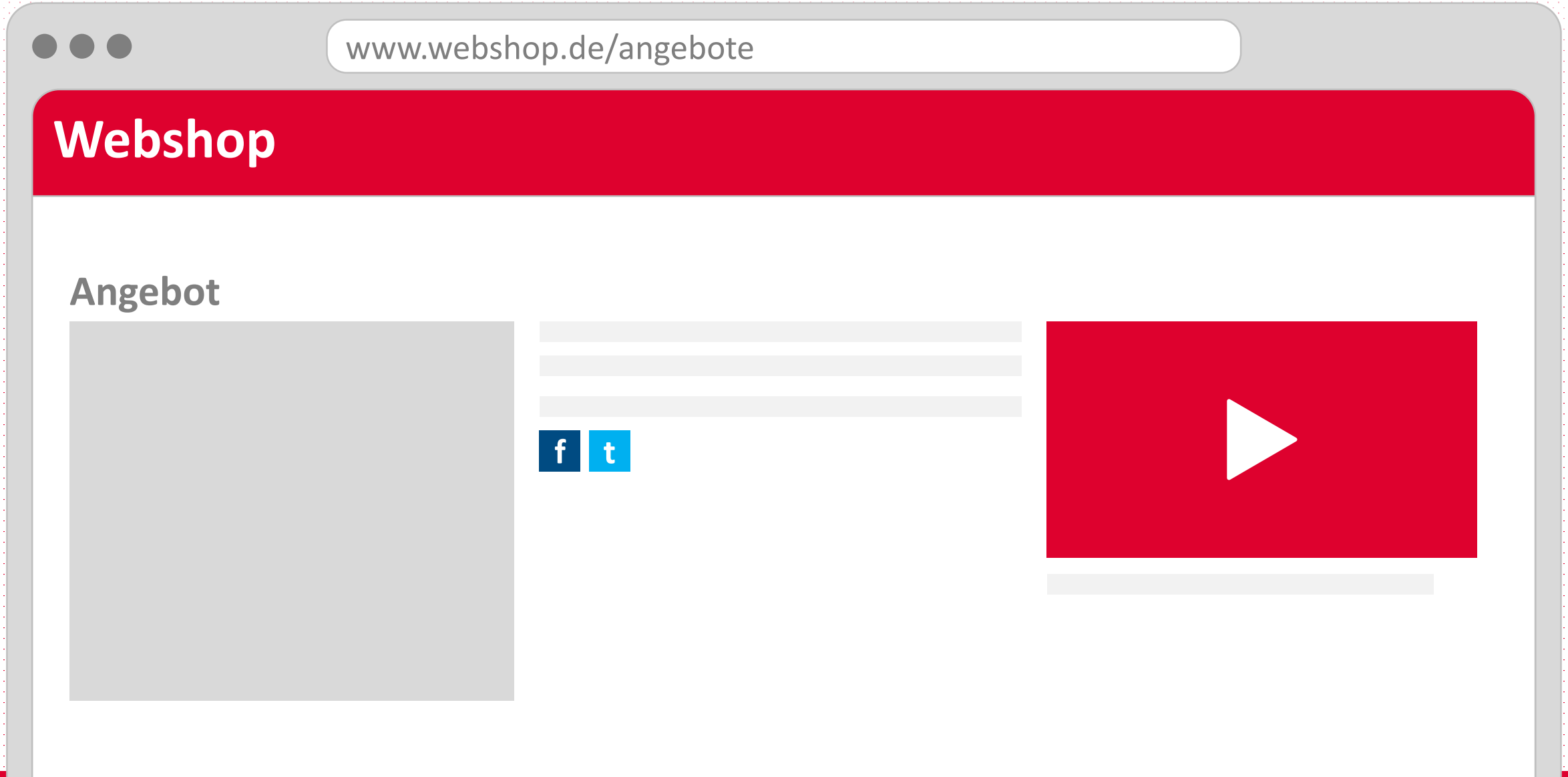
Webseiten-Tracking



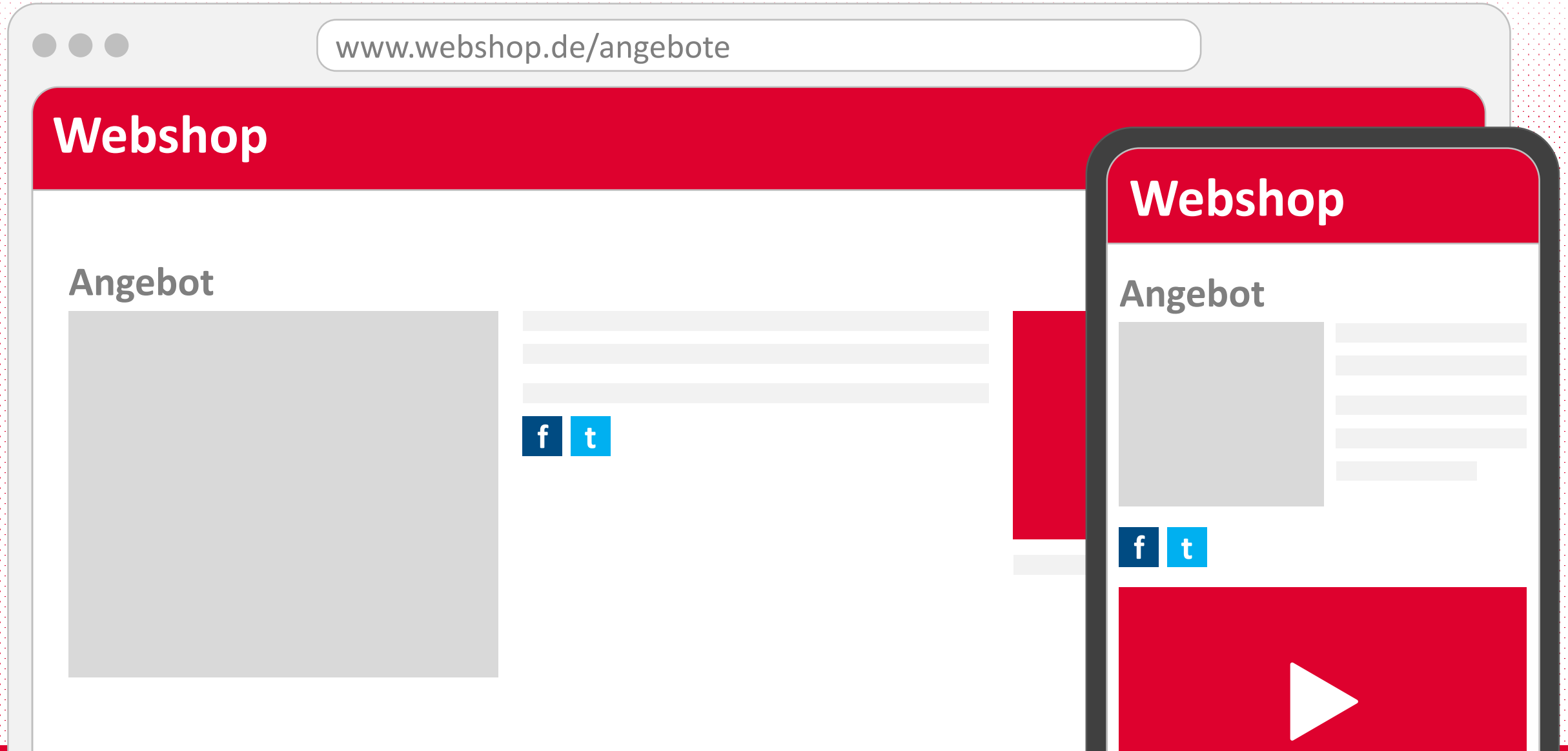
Wie funktioniert Webseiten-Tracking?



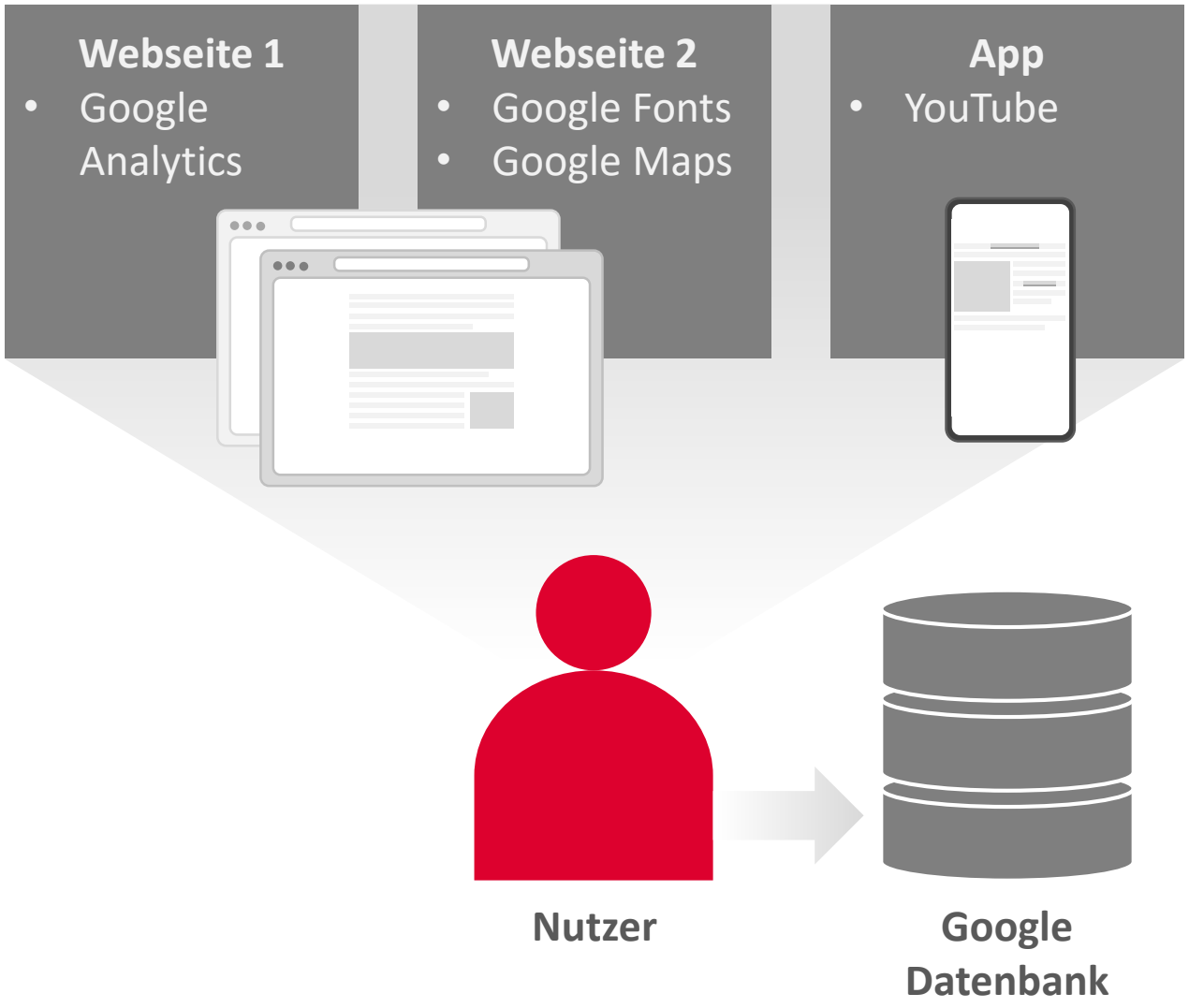
Wie funktioniert Webseiten-Tracking?



Wie funktioniert Webseiten-Tracking?



Wie funktioniert Tracking? – am Beispiel Google



- **Identifizierung** möglichst aller Nutzer
- **Verfolgen** der Nutzer über mehrere Webseiten und Apps
- **Auswerten** des Verhaltens und der Vorlieben der Nutzer

Tracking

E-Mail-Tracking

Was kann getrackt werden?

- **Öffnungsraten**
  - Wann und wie oft wurde die E-Mail geöffnet?
- **Klickraten**
  - Welche Links wurden geöffnet?
  - Wie oft wurden Links geöffnet?
- **Profilbildung**
  - Wo wurde die E-Mail gelesen?

Wie wird getrackt? – Tracking Pixel (Web-Beacon)

- Ist ein **grafisches Element**, dass in den Code von E-Mails eingebettet wird
- In der Regel 1x1 Pixel groß
- Einzigartige ID angefügt
- Für den Nutzer unsichtbar

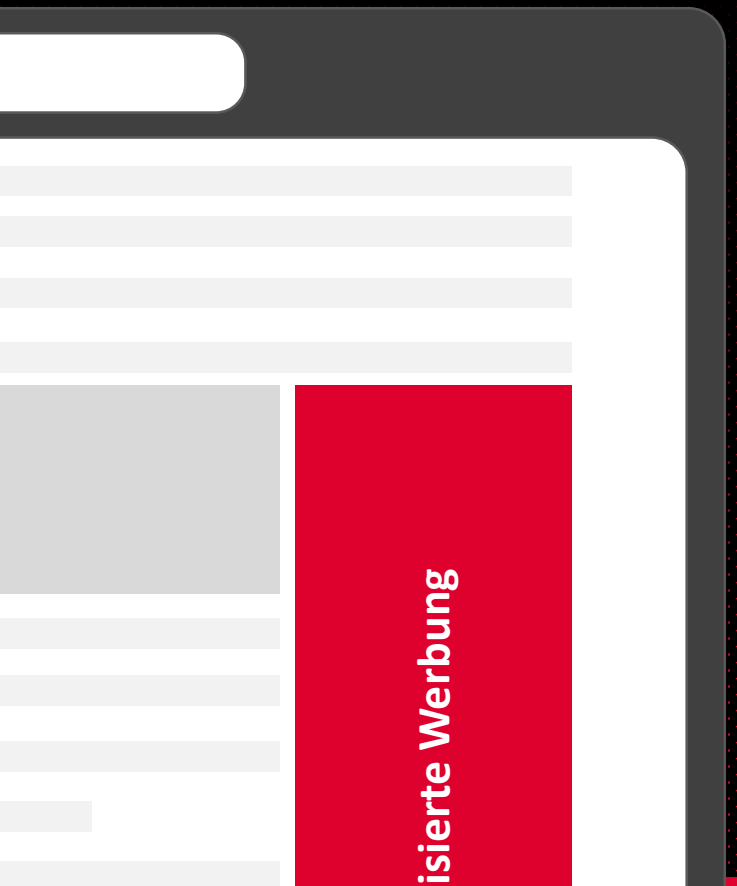
Wie wird getrackt? – Serverseitige Grafiken

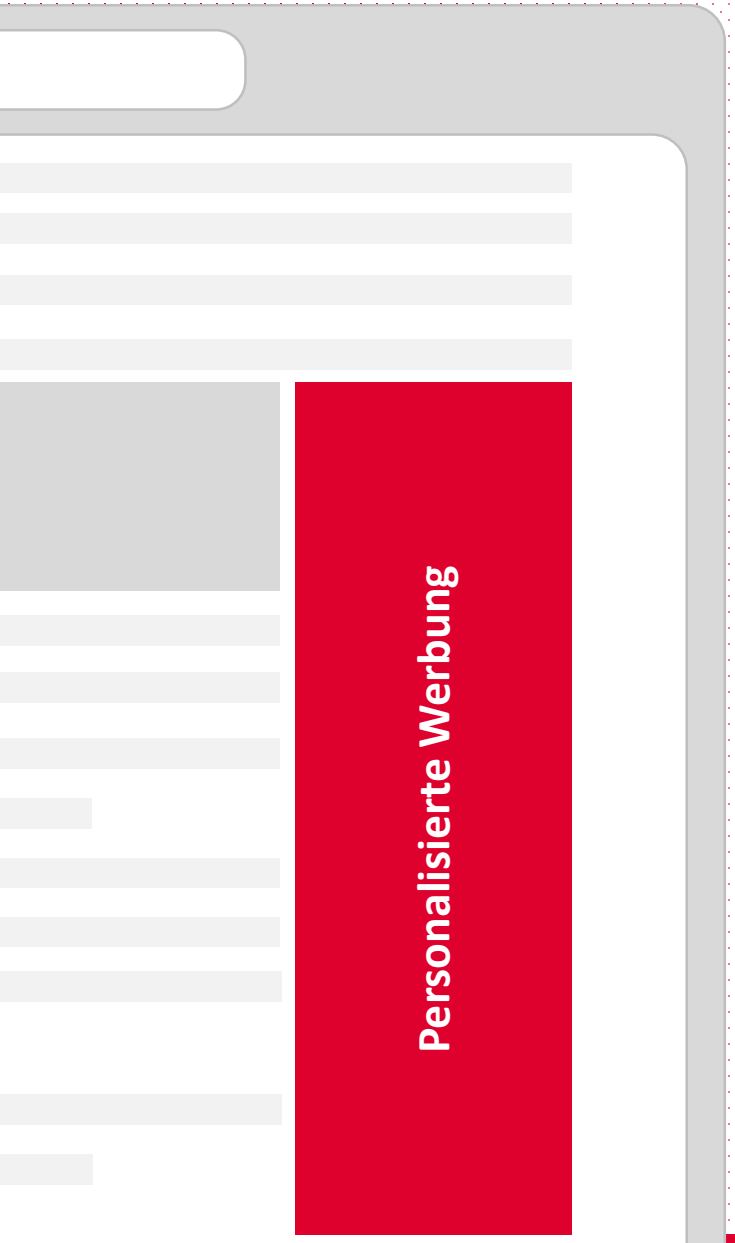
- Die Grafiken werden nicht mit der E-Mail versandt, sondern von einem Server nachgeladen
- Ggf. Parameter und einzigartige ID angefügt

Wie wird getrackt? – Tracking Links

- Sind URLs mit angehängten Parametern und/oder einzigartigen IDs, z. B. https://m.heise.de/foto/?wt_**ref**=https%3A%2F%2Fwww.heise.de&wt_**t**=1617819989855

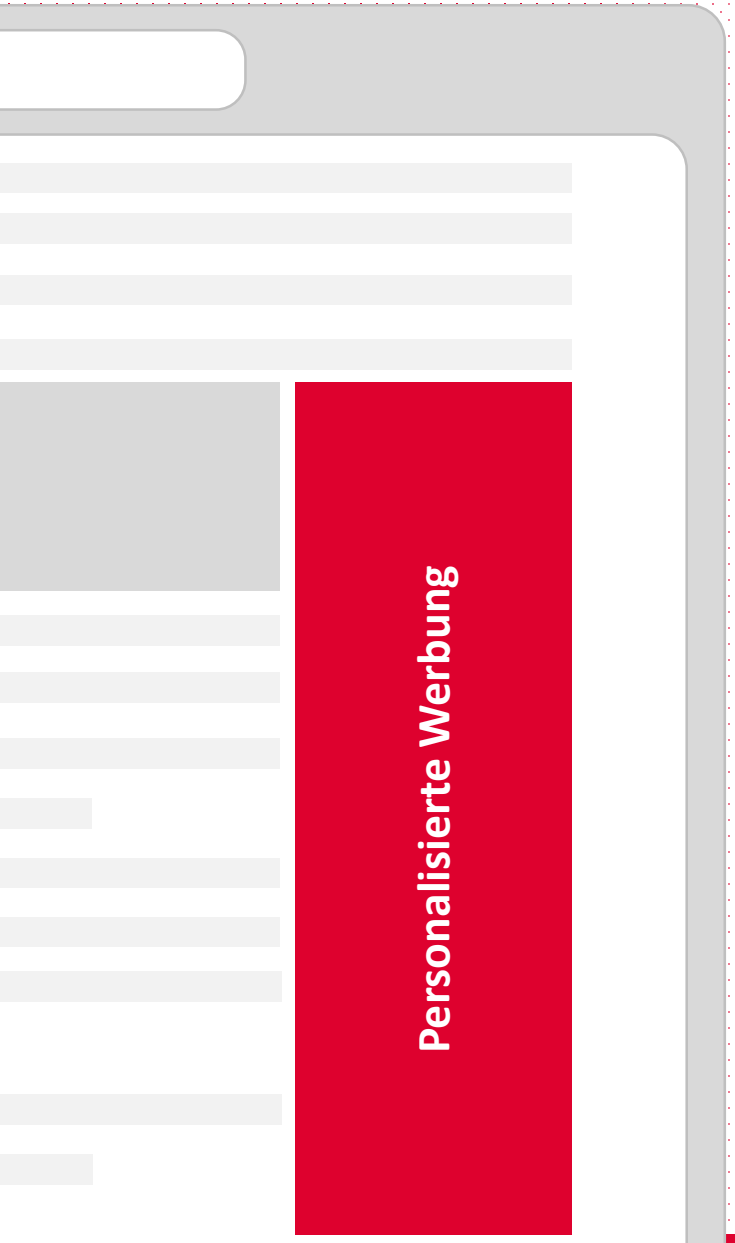
Profiling





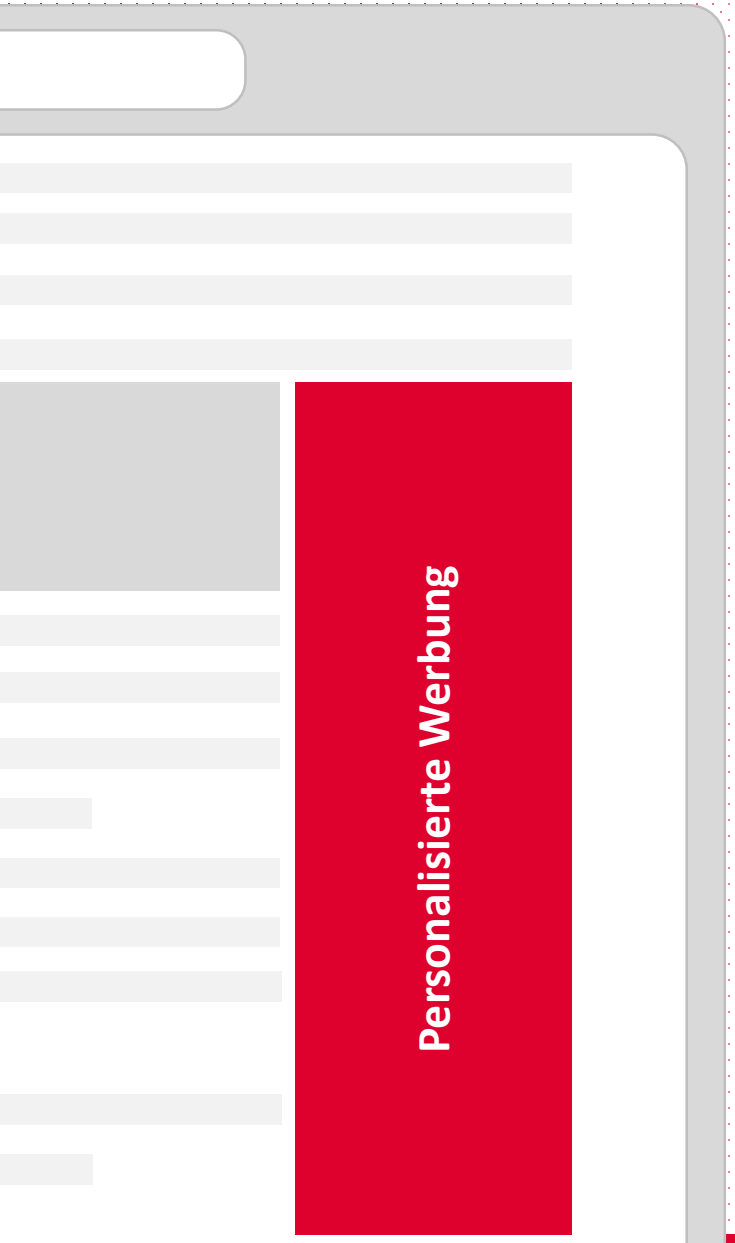
Vom Tracking zum Profiling

- **Profiling** ist die automatisierte Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person



Vom Tracking zum Profiling

- Insbesondere Analyse oder Prognose von Aspekten bezüglich:



Ziele von Profiling

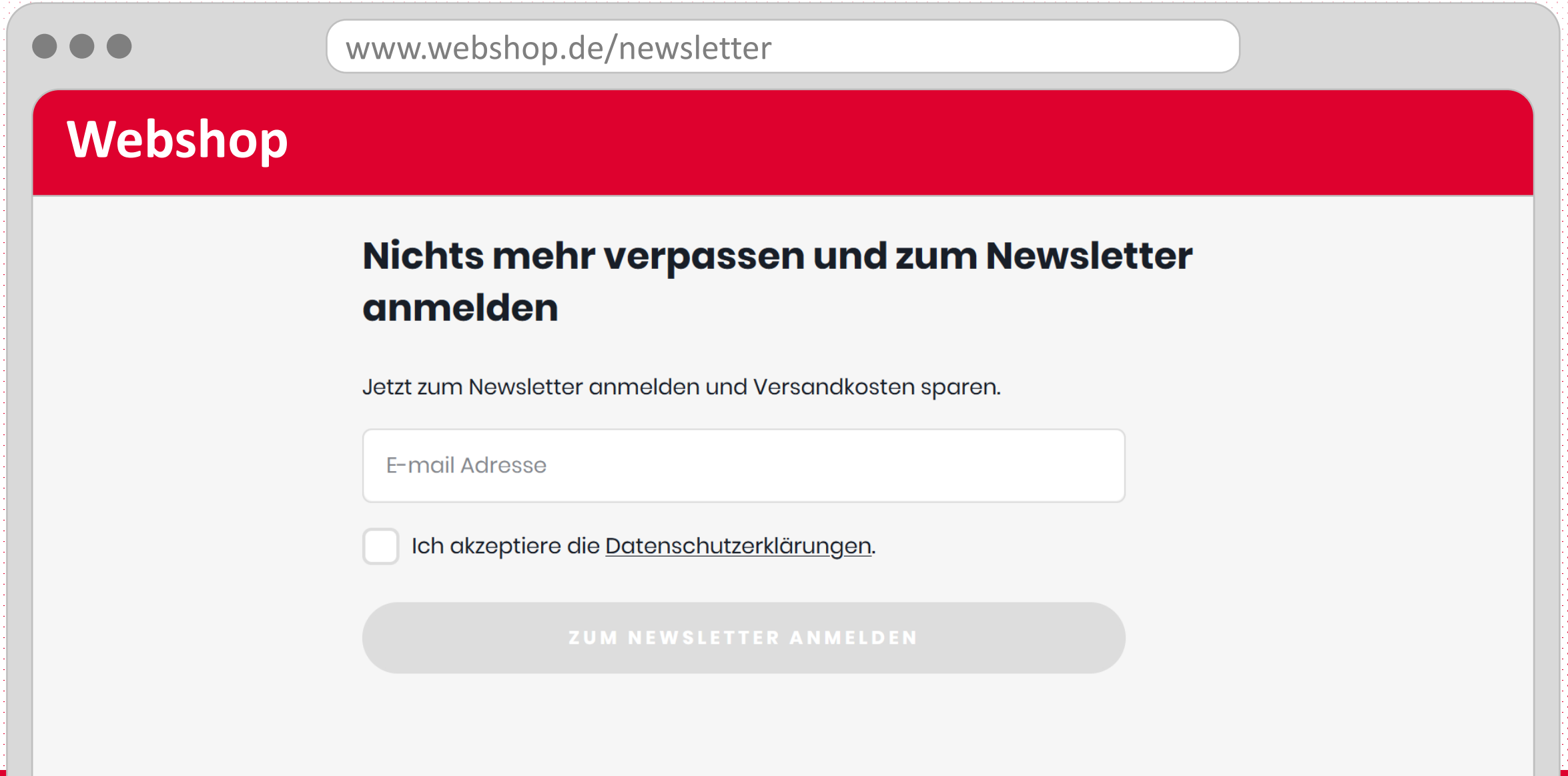
- Erstellung des Gesamtbildes einer natürlichen Person für bestimmte Zwecke
  - Zusammenführen von Daten
  - Analysieren von Daten durch Algorithmen
  - “Big Data”
- Scoring / Vorhersagen
  - Einordnen unter verschiedenen Aspekten
  - Bilden und Verwenden eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten
- Gezieltes und individuelles Ansprechen
- Beeinflussen von Entscheidungen

Rechtliche Risiken

Bisherige Umsetzung

- Oft wird nur eine Einwilligung für den **Empfang** der E-Mails eingeholt
- **Nicht** aber für **Tracking** und **Profiling** sowie den **Zweck** der Datenverarbeitung
- Mangelhafte Information des Betroffenen
- Falsche oder unvollständige Rechtsgrundlage

Praxisbeispiel



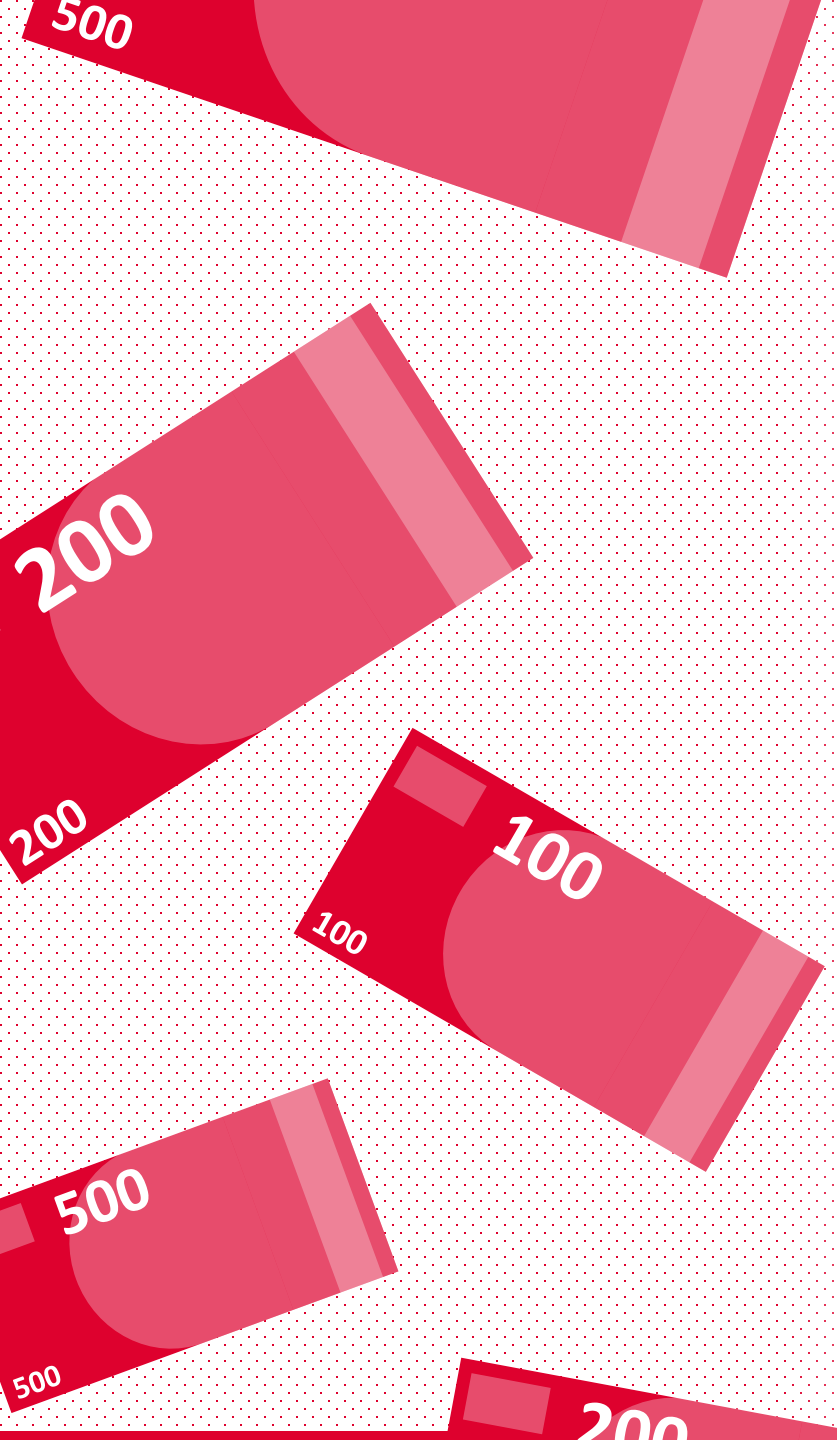
Beispiel

www.webshop.de/datenschutz

Webshop

Datenschutzerklärung

Wir weisen dich daraufhin, dass wir bei Versand des Newsletters dein Nutzerverhalten auswerten. Für diese Auswertung beinhalten die versendeten E-Mails sogenannte Web-Beacons bzw. Tracking-Pixel unseres Email-Versanddienstleisters, sowie unserer Web Analytics Technologie. Diese Technologie erlaubt es uns, dein Öffnungs- und Klickverhalten zu erfassen. Darüber hinaus können diese Daten mit dem Verhalten dieses pseudonymen Profils auf unserer Webseite zusammengeführt werden. Mit den so gewonnenen Daten erstellen wir ein Nutzerprofil, um dir den Newsletter auf deine individuellen Interessen zuzuschneiden. Dabei erfassen wir, wann du unseren Newsletter liest, welche Links du in diesem anklickst und folgern daraus deine persönlichen Interessen. Diese Daten verknüpfen wir mit von dir auf unserer Webseite getätigten Handlungen.

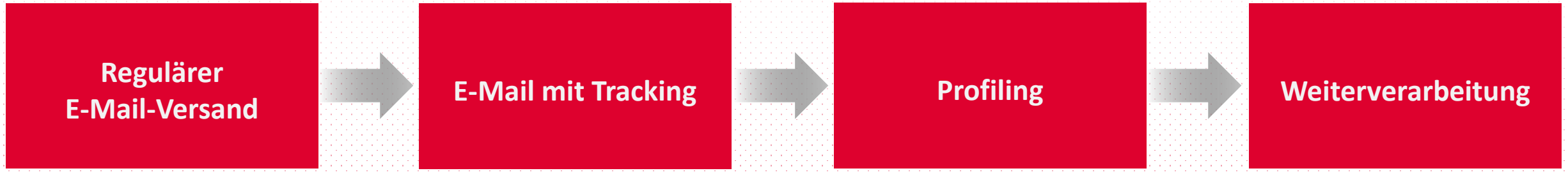


Mögliche Folgen

- Bußgeld
  - Art. 83 Abs. 5 DSGVO
    - Bis zu 20 Mio. € (je Verstoß) oder
    - Bis zu 4% des weltweit erzielten Jahresumsatzes
  - § 28 TTDSG
    - Bis zu 300.000 €
- Schadensersatz
  - Art. 82 Abs. 1 DSGVO
  - § 823 Abs. 1 BGB
- Beseitigungs- & Unterlassungsanspruch
  - §§ 8 Abs. 1, 7 Abs. 1, Abs. 2 Nr. 2 UWG
- Imageverlust

Rechtskonforme Gestaltung

Rechtskonforme Gestaltung



Rechtskonforme Gestaltung

E-Mail-Versand

Rechtskonformer E-Mail-Versand

- Rechtsgrundlage, Art. 6 Abs. 1 DSGVO
  - Aktive Einwilligung
  - Vertrag
  - Berechtigtes Interesse
- Verarbeitung personenbezogener Daten
- Zu einem bestimmten Zweck

Exkurs: Wettbewerbsrechtliches Einwilligungserfordernis

- § 7 Abs. 2 Nr. 2 UWG: Unzumutbare Belästigung
- Ausnahme:
  - Zusammenhang mit Verkauf von Waren oder Dienstleistungen
  - Direktwerbung für eigene ähnliche Waren oder Dienstleistungen
  - Kein Widerspruch
  - Hinweis auf Widerspruchsrecht
- Einwilligungspflicht besteht auch bei berechtigtem Interesse gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO

Rechtskonforme Gestaltung

Tracking

Was ist die Rechtsgrundlage für Tracking?

DSGVO	TTDSG
Schutz personenbezogener Daten	Schutz von Endgeräten
Art. 6 Abs. 1 lit. a DSGVO (Einwilligung)	**§ 25 TTDSG (Einwilligung)**
Art. 6 Abs. 1 lit. b DSGVO (Vertrag)	
Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)	

DSGVO oder TTDSG?

- Kollisionsregel des Art. 95 DSGVO zur E-Privacy Richtlinie
  - **Vorrang des TTDSG** bei Verarbeitung in Verbindung mit der Bereitstellung **öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen**

→ Dienste, deren Nutzen darin besteht, Information und Kommunikation auf elektronischem Wege zu vermitteln, insbesondere via Internet

z. B. E-Mail, Videokonferenztools, Cookies

DSGVO oder TTDSG?

§ 25 Abs. 1 S. 1 TTDSG

1. Die **Speicherung von Informationen** in der Endeinrichtung des Endnutzers oder
2. der der **Zugriff auf Informationen**, die bereits in der Endeinrichtung gespeichert sind,

sind **nur zulässig**, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen **eingewilligt** hat.

Gibt es Ausnahmen?

§ 25 Abs. 2 Nr. 2 TTDSG

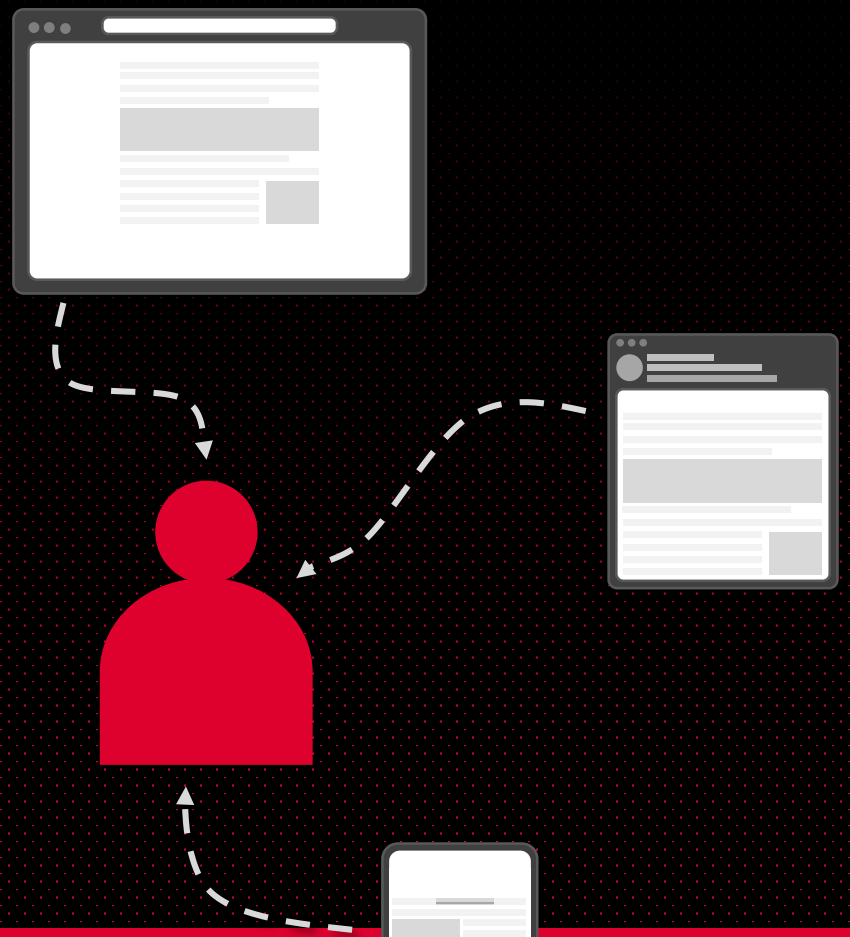
Die Einwilligung ist nicht erforderlich, wenn der Zugriff auf Informationen **unbedingt erforderlich** ist, um **einen vom Nutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen**.

- **Nicht einschlägig**, da Tracking nicht unbedingt erforderlich ist.

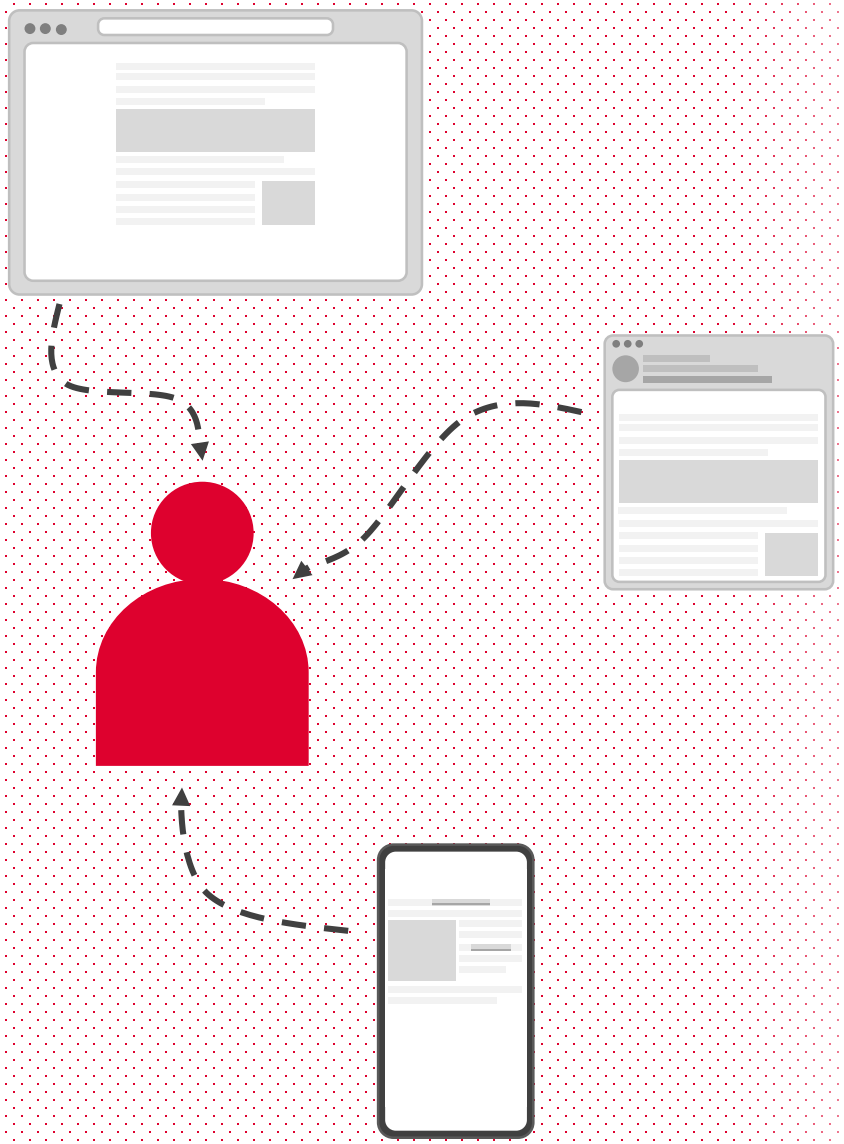
→ **Einwilligung ist für Tracking grundsätzlich erforderlich!**

Rechtskonforme Gestaltung

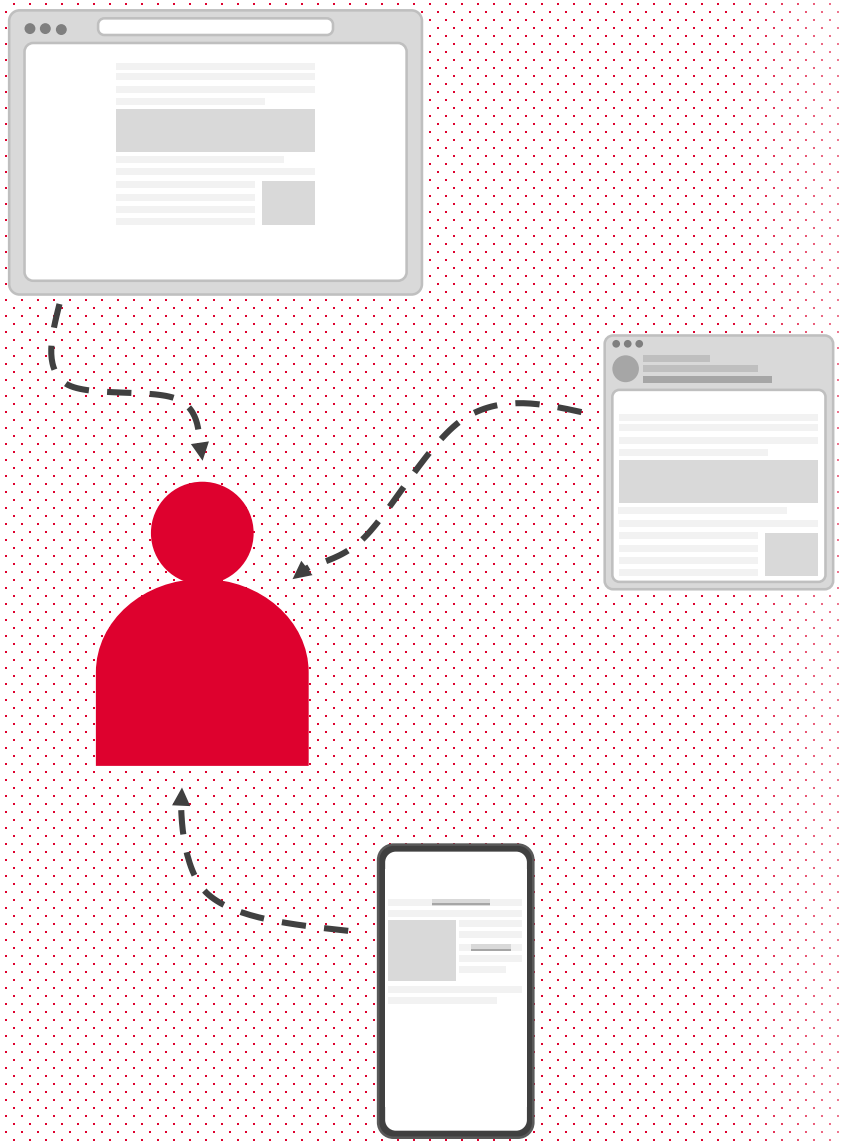
Profiling



Was ist die Rechtsgrundlage für Profiling?

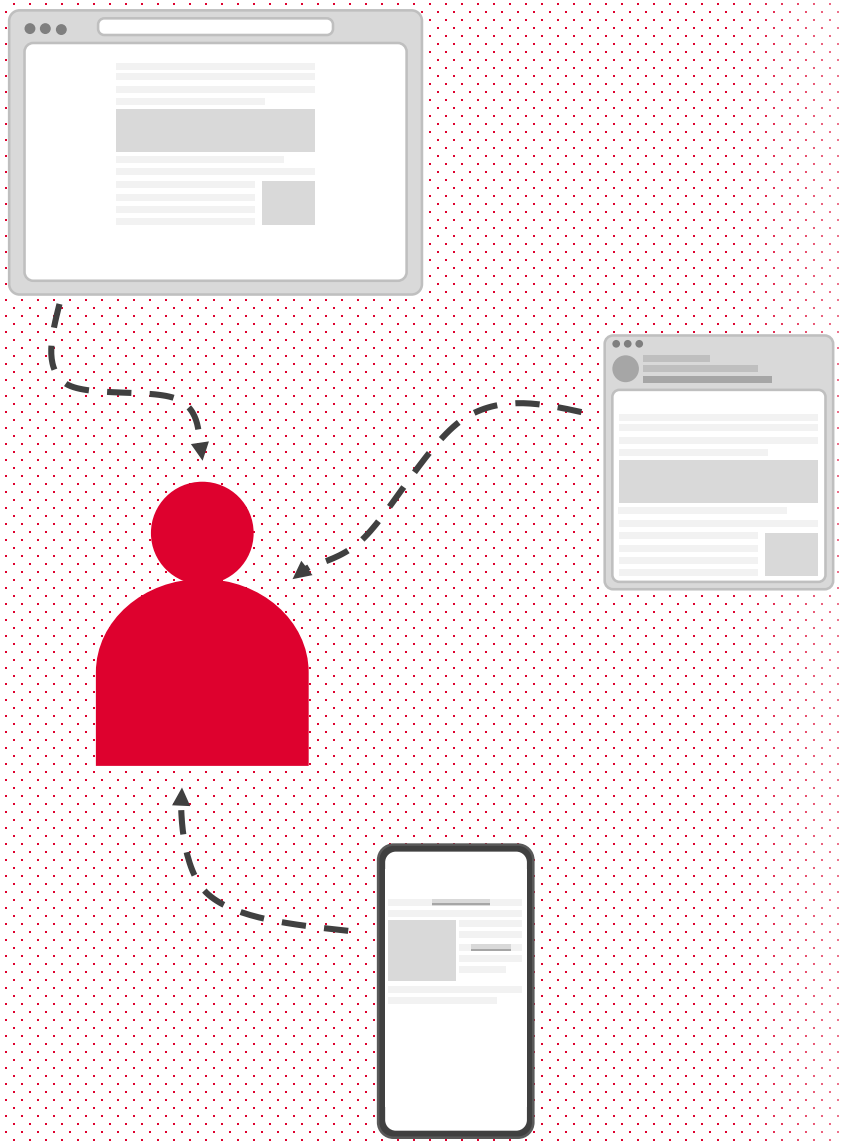


DSGVO	TTDSG
Schutz personenbezogener Daten	Schutz von Endgeräten
Art. 6 Abs. 1 lit. a DSGVO (Einwilligung)	§ 25 TTDSG (Einwilligung)
Art. 6 Abs. 1 lit. b DSGVO (Vertrag)	
Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse)	



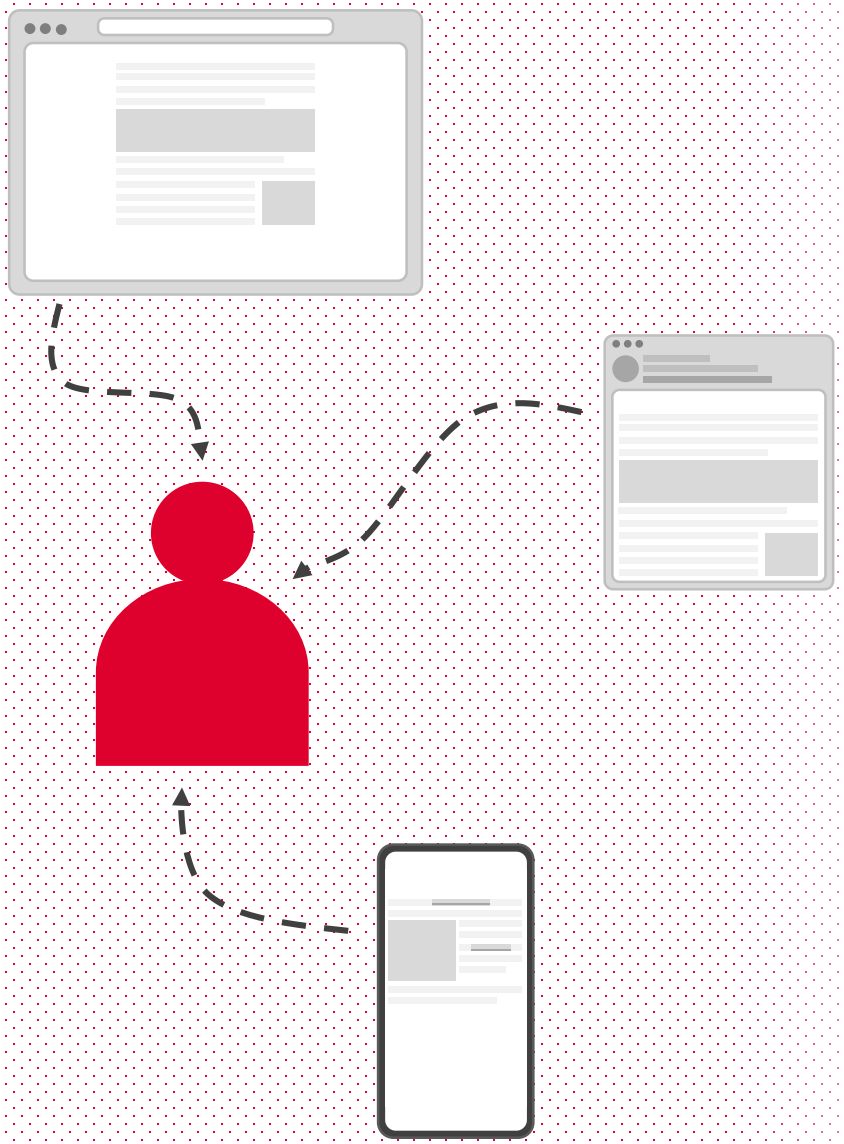
DSGVO oder TTDSG?

- Kollisionsregel des Art. 95 DSGVO
  - TTDSG nur Rechtsgrundlage für Zugriff auf Öffnungs- und Klickraten auf Endgeräten der Nutzer
- DSGVO ist hingegen Rechtsgrundlage für deren Speicherung in Nutzerprofilen beim Empfänger



Rechtsgrundlagen nach der DSGVO

- Einwilligung
- Zur Erfüllung eines Vertrag
- Berechtigtes Interesse
  - ggfs. betriebswirtschaftliche Interessen, wenn die Interessen der Adressaten am Schutz ihrer Daten diese Interessen nicht überwiegen (ErwG 47 DSGVO)



Anforderungen an die Einwilligung

- Informiert

  Welchen Zweck verfolgen die Werbemaßnahmen im Einzelnen?

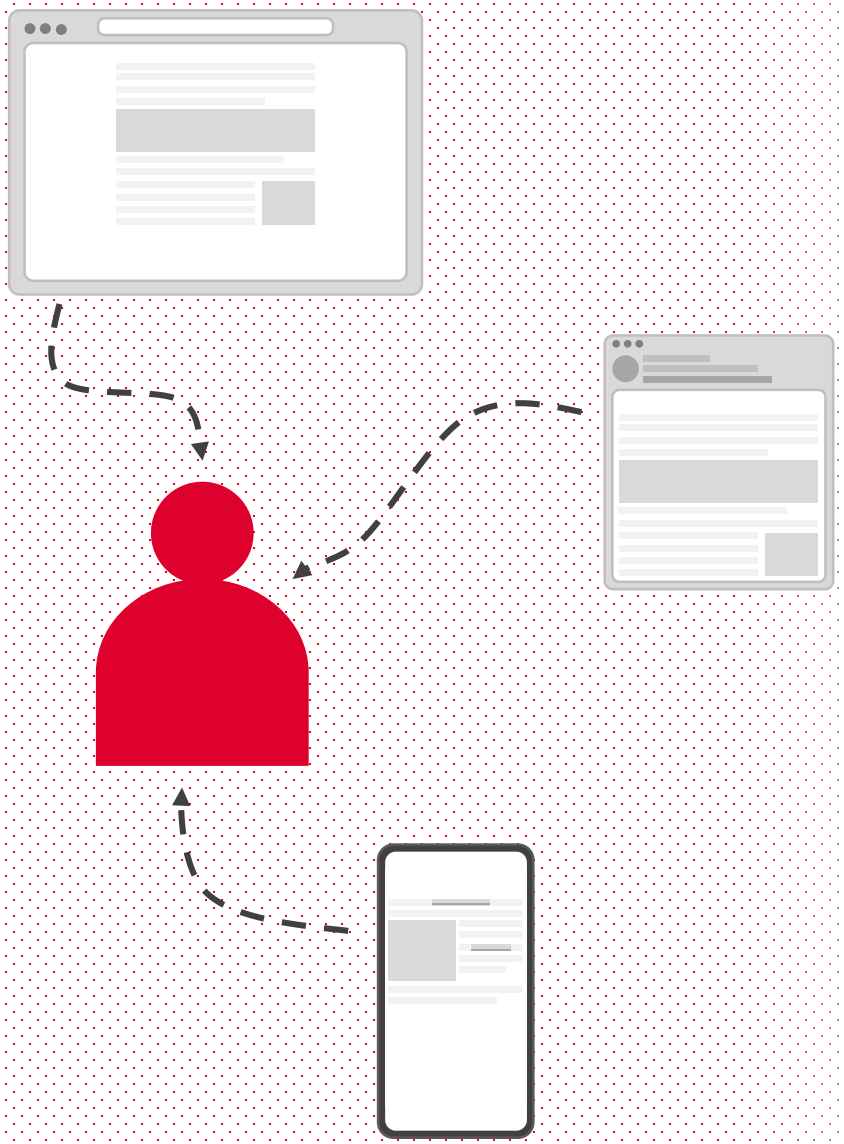
- Separat

  Welche einzelnen Werbemaßnahmen werden mit der Einwilligung abgedeckt?

- Eindeutige bestätigende Handlung

  Der Betroffene muss aktiv zustimmen

- Freiwillig
- Ablehnung muss möglich sein
- Widerruf der Einwilligung muss jederzeit möglich sein



Beispiel einer rechtskonformen Einwilligung

- Klare und umfassende Informationen über
  - Zweck der Datenverarbeitung
  - Verwendung von Tracking
  - Verwendung von Profiling
  - Hinweis auf das Widerrufsrecht
  - Hinweis auf die Datenschutzerklärung
  - Aktive und freiwillige Einwilligung

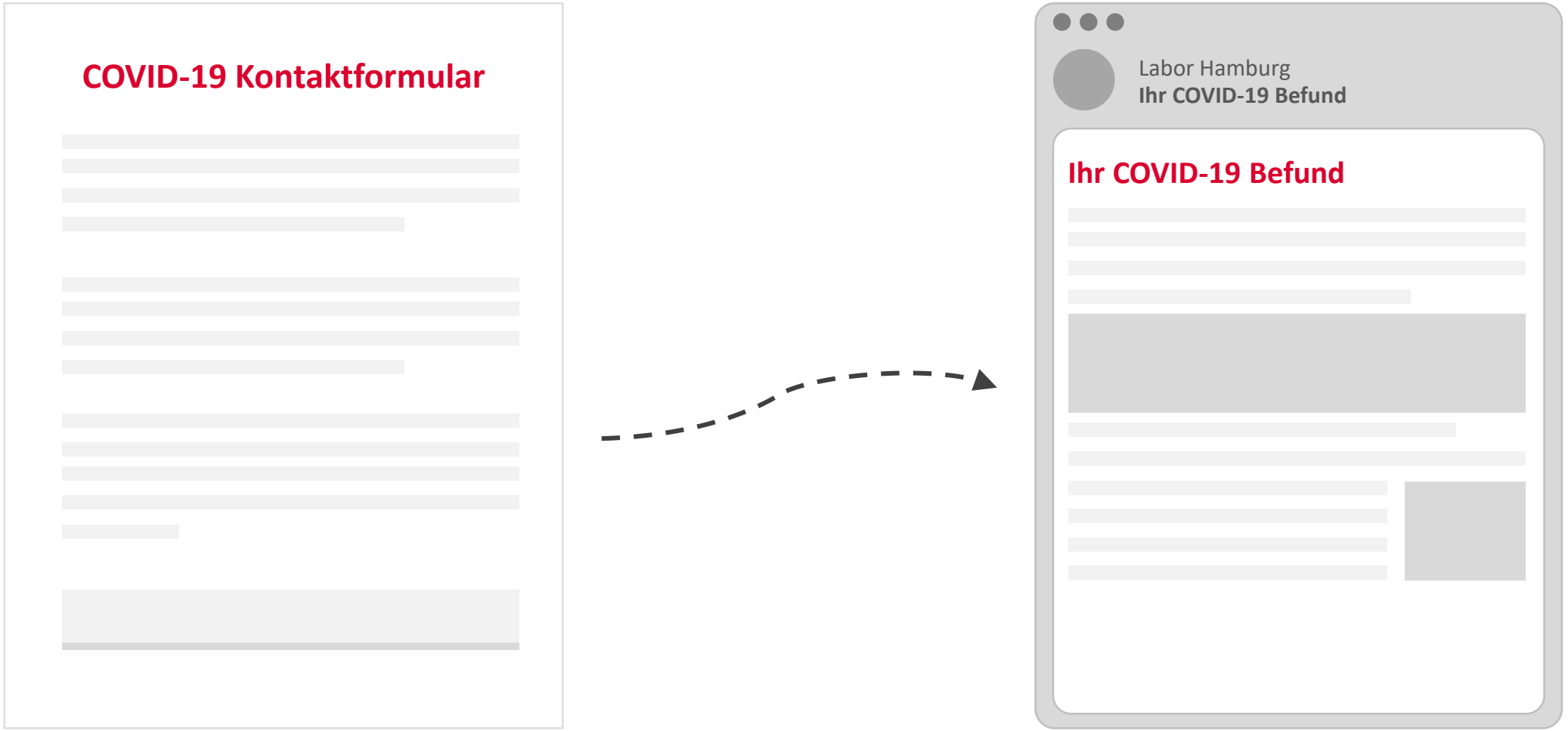
Formen der Einwilligung

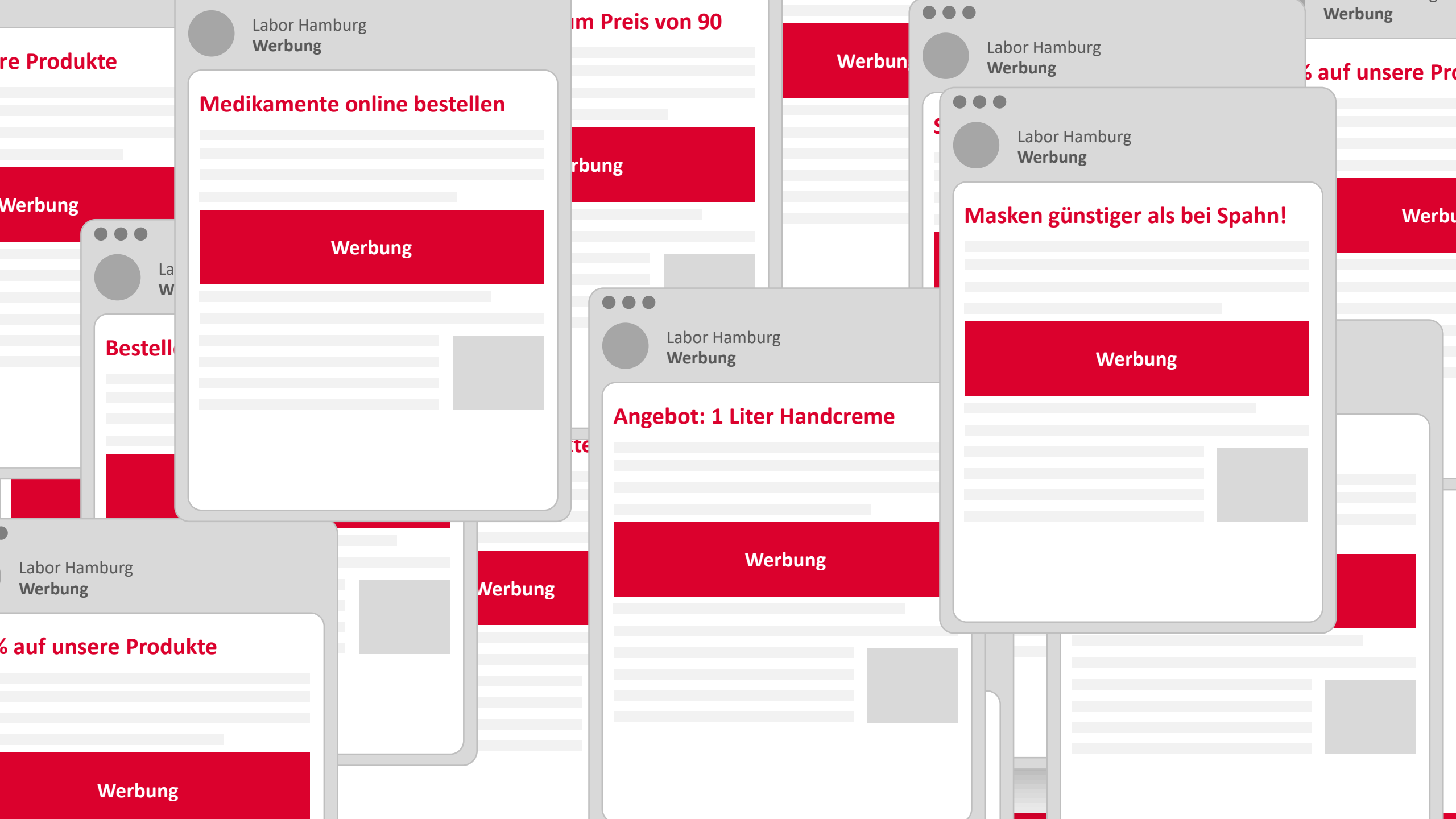
UWB (Wettbewerbsrecht)	DSGVO (Datenschutzrecht)	
Einwilligung bei Werbung	Einwilligung in die Datenverarbeitung	Einwilligung in Tracking und Profiling
§ 7 Abs. 2 Nr. 2 UWG	Art. 6 Abs. 1 lit. a DSGVO	§ 25 TTDSG
		Art. 6 Abs. 1 lit. a DSGVO

Rechtskonforme Gestaltung

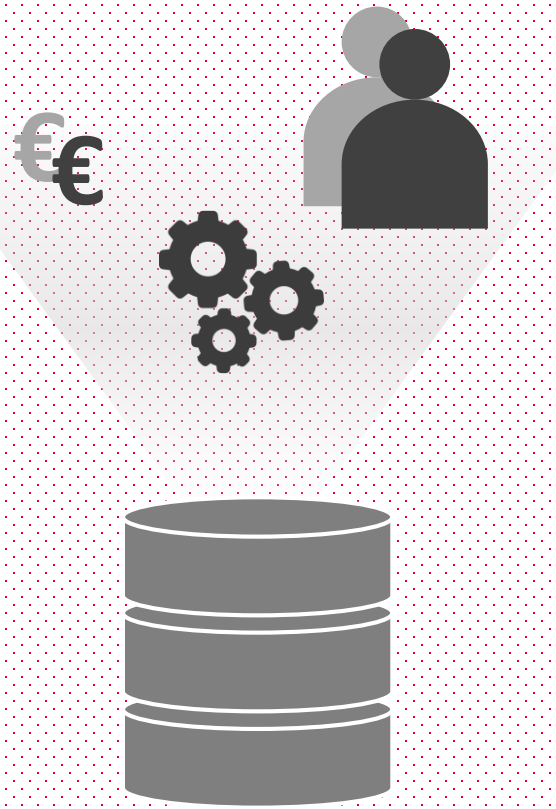
Weiterverarbeitung

Beispiel


COVID-19 Kontaktformular
Labor Hamburg
Ihr COVID-19 Befund
Ihr COVID-19 Befund


Labor Hamburg
Werbung
Medikamente online bestellen
Werbung
Labor Hamburg
Werbung
Angebot: 1 Liter Handcreme
Werbung
Labor Hamburg
Werbung
Masken günstiger als bei Spahn!
Werbung
Labor Hamburg
Werbung
% auf unsere Produkte
Werbung

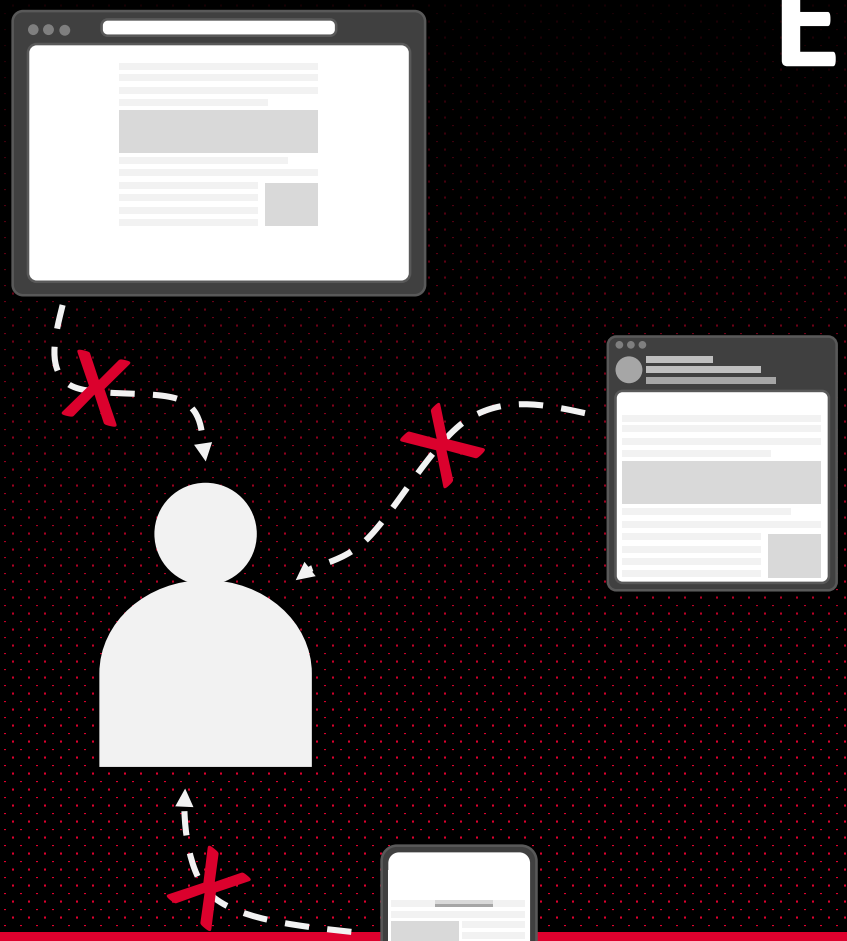
Weiterverarbeitung



- Verarbeitung zu einem **anderen Zweck**
- Voraussetzungen des Art. 6 Abs. 4 DSGVO
  - Ursprüngliche Rechtsgrundlage?
    - Einwilligung → Verarbeitung zu anderem Zweck möglich
  - Andere Rechtsgrundlage → Prüfung der Vereinbarkeit
- Information des Betroffenen über die Verarbeitung und das Widerspruchsrecht

Rechtskonforme Gestaltung

Einzelprobleme

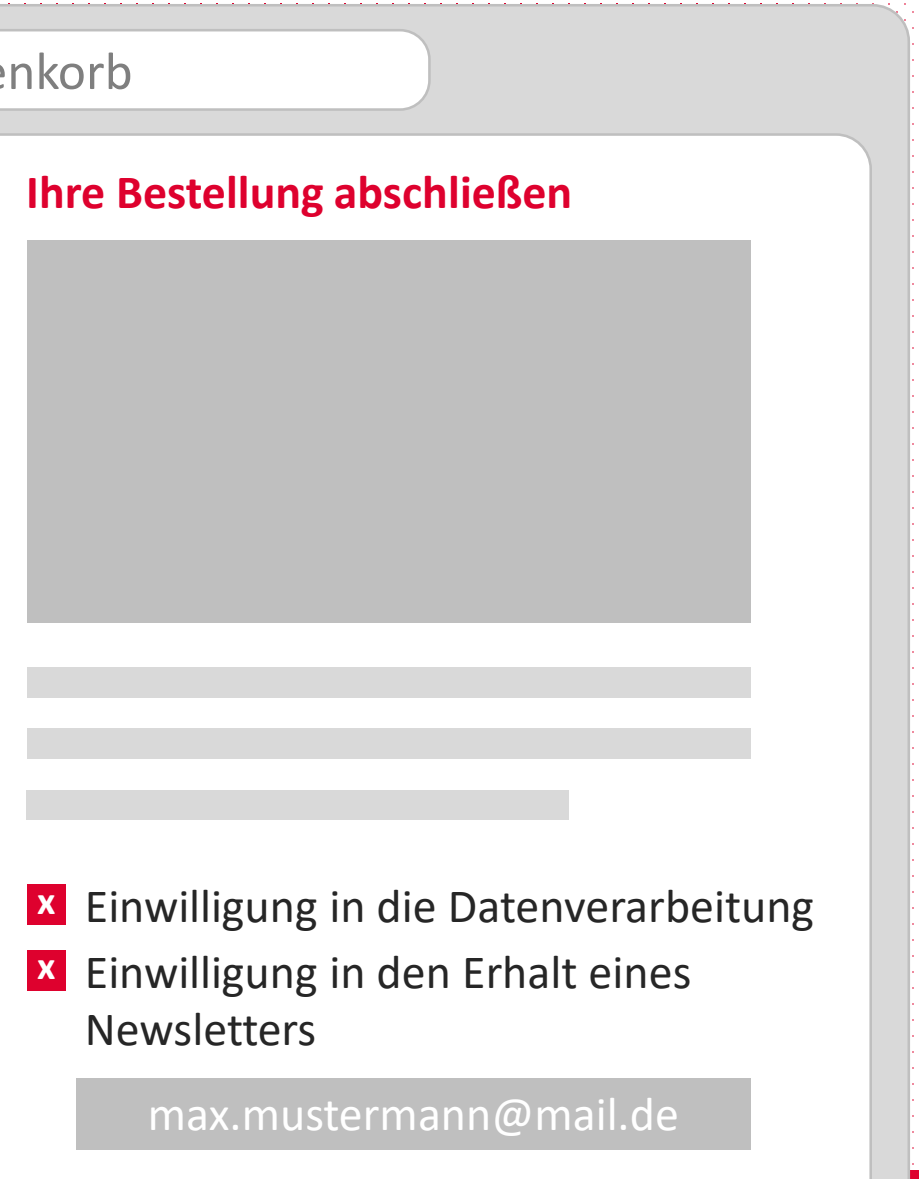


Wegfall der Rechtsgrundlage

- Wegfall durch:
  - Widerruf der Einwilligung (Art. 7 DSGVO)
  - Widerspruch gegen die Verarbeitung (Art. 21 DSGVO)
- Einwilligung wurde nicht eingeholt
  - Es darf kein Tracking und Profiling stattfinden
  - Es muss nachträglich eine Einwilligung eingeholt werden.
- Folgen für den Verarbeiter:
  - Daten dürfen nicht weiterverarbeitet werden
  - Löschung der Daten gem. Art. 5 und Art. 17 DSGVO

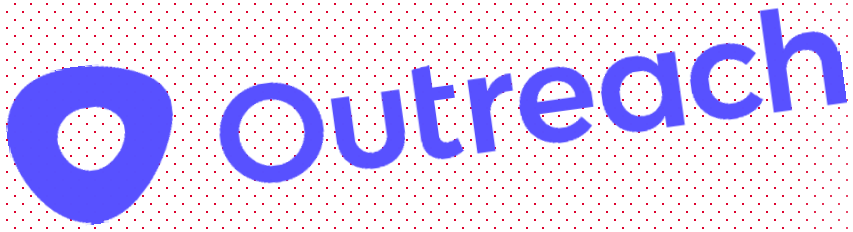
    u. a. Tracking-Links serverseitig deaktivieren

Kopplungsverbot



- Ableitung aus dem Grundsatz der Freiwilligkeit (Art. 7 Abs. 4 DSGVO)

  z. B. bei Einwilligung im Rahmen eines Abschlusses einer Bestellung
- Die Einwilligung muss freiwillig sein
- Nicht freiwillig, wenn sie zur Bedingung eines Vertragsschlusses gemacht wird



Versand und Tracking durch externe Marketing-Platformen

- Was sind Marketing-Plattformen?
- Ggfs. durch Anbieter in Drittstaaten?

  → Art. 44 ff. DSGVO
  - Wo werden die Daten gespeichert?
  - Wo hat das Unternehmen seine(n) Sitz(e)?
  - „Schrems II“-Urteil des EuGH beachten!

Rechtskonforme Gestaltung

Zwischenergebnis

E-Mail Tracking und Profiling müssen freiwillig und optional sein!

E-Mail Tracking und Profiling müssen freiwillig und optional sein!

- Aktive informierte freiwillige Einwilligung
- Transparenz bzgl. dem Zweck der Verarbeitung
- Echte Wahlmöglichkeit und Entscheidungsfreiheit
- Hinweis auf das Widerrufsrecht und die Datenschutzerklärung

E-Mail Tracking und Profiling müssen freiwillig und optional sein!

www.webshop.de/newsletter

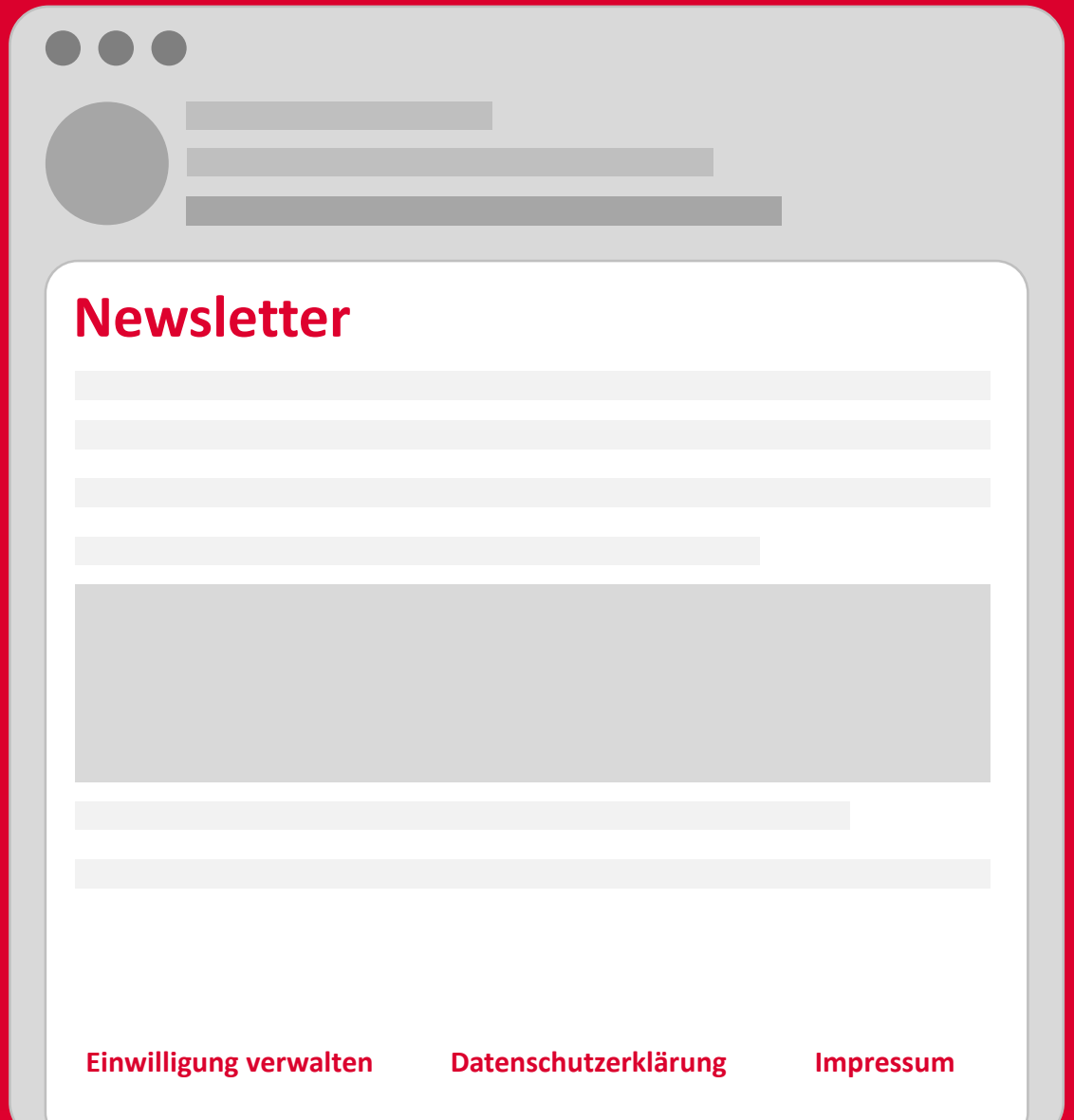
X Ja, ich möchte per E-Mail über aktuelle Produkte und Dienstleistungen von Webshop GmbH informiert werden.
Diese Produkte sind …

X Ja, ich möchte, dass diese Informationen auf meine persönlichen Interessen zugeschnitten sind.
Sofern Sie uns Ihre Einwilligung dazu geben, werden wir Ihr **Nutzerverhalten** auf unseren Web-Auftritten sowie innerhalb der von uns versendeten Newsletter **auswerten** und Ihrer E-Mail-Adresse/Ihrem Nutzerprofil innerhalb unserer Datenbank zuordnen. Wir speichern weiterhin Informationen über den von Ihnen verwendeten Browser und die vorgenommenen Einstellungen in Ihrem verwendeten Betriebssystem sowie Informationen zu Ihrer Internetverbindung, mit der Sie unsere Website erreichen. In dem an Sie versendeten Newsletter erhalten wir unter anderem **Empfangs- und Lesebestätigungen** sowie **Informationen über die Links, auf die Sie in unserem Newsletter geklickt** haben. Auch speichern wir, welche Bereiche Sie innerhalb unseres Web-Auftritts und in unseren Apps besucht haben. Durch das **Erstellen eines persönlichen Benutzerprofils** möchten wir unsere werbliche Ansprache auf Ihre Interessen ausrichten und unsere Angebote auf unserer Website für Sie optimieren.

Ihre Einwilligung können Sie jederzeit unter diesem Link oder mittels einer E-Mail an abmeldung@webshop.de widerrufen. Ihr Widerruf führt zur Löschung der von uns erhobenen Daten.
Weitere Informationen erhalten Sie in unseren Datenschutzhinweisen.

Anmelden

E-Mail Tracking und Profiling müssen freiwillig und optional sein!



- Änderung und Widerruf müssen genauso einfach sein, wie die Einwilligung selbst

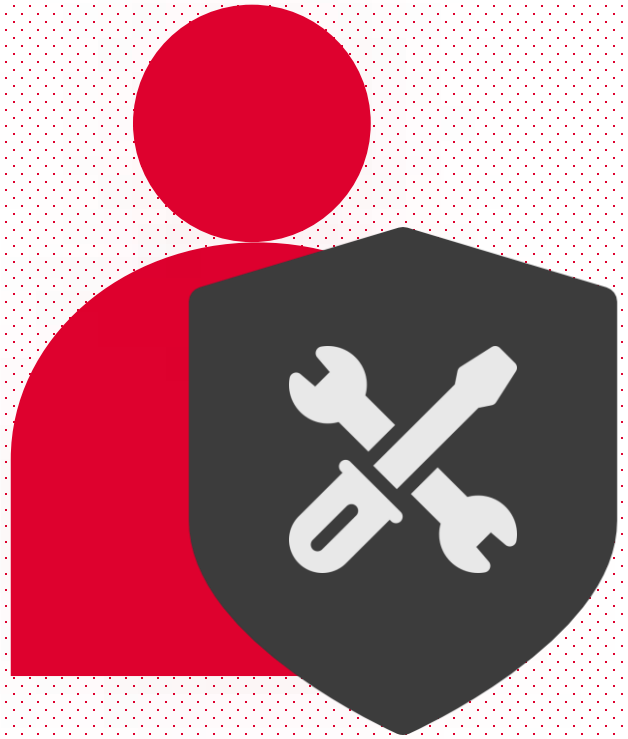
- Maßnahmen
  - Einstellung muss für zukünftige E-Mails übernommen werden bzw. das erstelle Nutzerprofil muss gelöscht werden
  - Tracking-Links alter E-Mails müssen deaktiviert werden

Persönliche Schutzmaßnahmen

Rechtliche Schutzmaßnahmen

- Die Einwilligung widerrufen, Art. 7 DSGVO
- Der Verarbeitung widersprechen, Art. 21 DSGVO
  - Datenverarbeitung zur Wahrung des berechtigten Interesses, Art. 6 Abs. 1 S. 1 lit. f DSGVO
  - Datenverarbeitung zu Zwecken der Direktwerbung, Art. 21 Abs. 2 DSGVO
  - Datenverarbeitung im Rahmen des Profilings, Art. 22 DSGVO
- Einen Antrag auf Löschung der personen-bezogenen Daten stellen, Art. 17 DSGVO
- Eine Beschwerde an die Aufsichtsbehörde erheben, Art. 77 DSGVO

Technische Schutzmaßnahmen



- Konfiguration des Mail-Clients
  - Nachladen von Grafiken unterbinden
- Tools
  - E-Mail-Client Tracking-Schutz nutzen
  - Blocker-Erweiterungen/Plugins

    z. B.Ugly Email, Trocker, Privacy Badger
  - VPN nutzen

Was bleibt?

- Abmeldung von Mailingliste deaktiviert in den meisten Fällen nicht das Tracking und Profiling
- Blockieren von Trackern ist nicht dasselbe wie das Deaktivieren von Tracking

Vielen Dank für Ihre Aufmerksamkeit!

Christian Blaicher

christian.blaicher@secorvo.de

Friederike Schellhas-Mende

friederike.schellhas-mende@secorvo.de