Good Advertising Kodex

Präambel

„Good Advertising“ ist ein Konzept für vertrauenswürdige Datennutzung in der Medien- und Werbewirtschaft. Die digitale Werbewirtschaft ist eine Grundvoraussetzung für eine vielfältige Medienlandschaft in Europa und steht in einem Spannungsfeld zwischen dem Schutz von Daten und der Notwendigkeit ihrer Nutzung zum Erhalt und zur Entwicklung wettbewerbsfähiger Geschäftsmodelle. Vor diesem Hintergrund investiert „Good Advertising“ bewusst in das Vertrauen von Nutzern, Markt und Politik.

Vertrauen durch integre Media- und Datenwertschöpfung

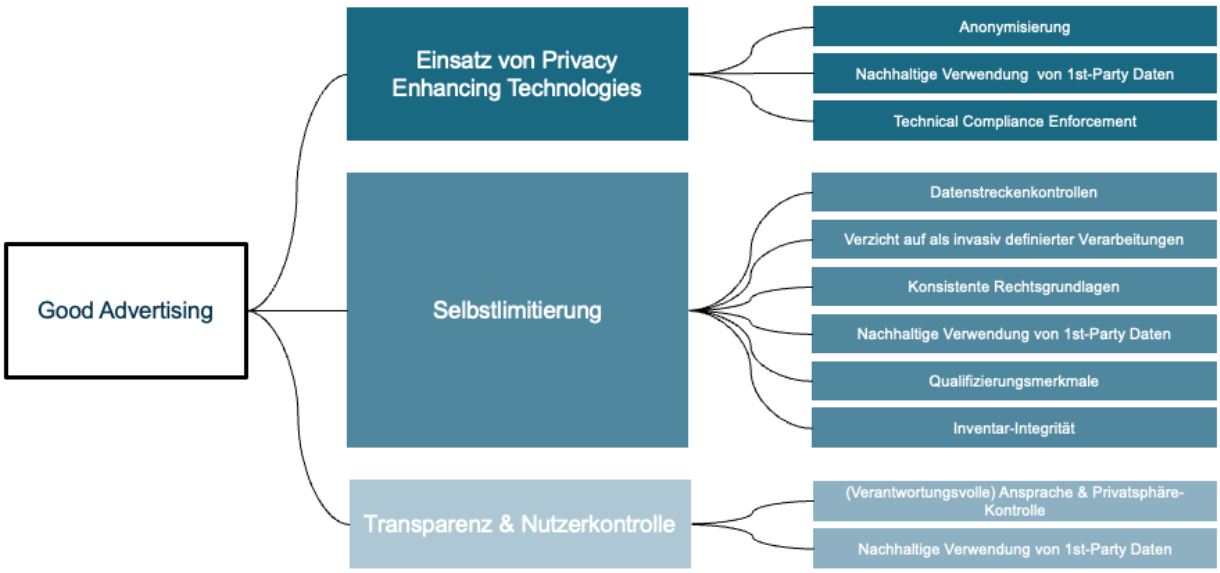
„Good Advertising“ strebt einen Rahmen – ausgedrückt in einem Verhaltenskodex – für verantwortungsvolle Datennutzung, Stärkung des Nutzervertrauens und Kontrolle von Zugang, Fluss und Verwendung von Daten an.

Der Kodex

Grundlage von „Good Advertising“ ist ein Stufenplan zur industrieweiten Entwicklung und Umsetzung eines Kodex von klar definierten und praktischen Verhaltensregeln. Eine erste Stufe bilden verantwortliche Praktiken, die Unterstützer bereits heute individuell umsetzen – etwa ein ausgewogener Umfang der Datennutzung und deren Kontrolle, ein Verzicht auf als invasiv wahrgenommene Verarbeitungen sowie eindeutige Wahlmöglichkeiten für Konsumenten.

Struktur von „Good Advertising“

Die folgende Übersicht zeigt die Struktur von „Good Advertising“ und ordnet die zentralen Handlungsfelder. Sie verdeutlicht, wie sich die nachfolgenden und zukünftigen Verhaltensregeln in eine übergreifende Struktur einbetten und welche Ansätze verfolgt werden.



Begriffe und Abkürzungen

Zur besseren Lesbarkeit werden im Kodex einzelne branchenübliche Fachbegriffe verwendet. Die nachstehenden Definitionen werden dem Kodex zugrunde gelegt; weiterführende Spezifikationen, insbesondere zur Umsetzung, können im technischen Annex enthalten sein.

- **Vendor (Anbieter):** Unternehmen, deren Technik in das digitale Angebot eingebunden ist (z. B. für Auslieferung, Messung oder Personalisierung von Werbung) und die dabei Daten verarbeiten und Endgerätezugriffe vornehmen. Sie nehmen typischerweise an einem standardisierten Privacy-/Consent-Framework teil.
- **Custom Vendor:** Anbieter, der nicht an einem standardisierten Framework hinsichtlich Privatsphäre-Einstellungen und deren Signalisierung teilnimmt und daher individuell konfiguriert/behandelt werden muss.
- **CMP (Consent-Management-Plattform):** Software-Komponente, die in digitalen Diensten verbaut ist. Erlaubt es Nutzern Privatsphäre-Einstellungen vorzunehmen und digitalen Diensten insbesondere die Ansprache bzgl. der Erteilung von Einwilligungen. Speichert Einstellung und kann diese – sofern durch ein eingesetztes Privacy-/Consent-Framework oder die eigene technische Implementierung vorgesehen – als technisches Signal an eingebundene Anbieter übermitteln.

- **SSP (Supply-Side-Plattform):** Vendor, mit der ein Publisher Werbeplätze anbietet und verkauft (z. B. in Auktions-/Programmatic-Umfeldern).
- **Supply Path (Lieferkette):** Die „Kette" der Stationen, über die ein Werbeplatz verkauft wird (z. B. Publisher → Plattform(en) → Zwischenhändler → Käufer).
- **Reseller (Wiederverkäufer):** Beteiligte, die im Auftrag oder als Zwischenhändler Werbeinventar weiterverkaufen.
- **Privacy-/Consent-Framework:** Branchenstandard, der definiert, wie Verwendungszwecke, Datenkategorien, Endgerätezugriffe und Verantwortliche verständlich beschrieben werden und wie Nutzersignale (z. B. Einwilligungen) technisch einheitlich an Anbieter übermittelt werden (z. B. TCF, GPP).
- **Purpose (Verwendungszweck):** Ein in der CMP ausgewiesener Verwendungszweck, für den Daten verarbeitet werden (z. B. „Messung", „Personalisierung").
- **SDK:** Software-Komponente, die in eine App eingebunden wird und dort Funktionen bereitstellt (z. B. Werbung, Messung) und dabei Daten verarbeitet und Endgerätezugriffe vornimmt.
- **WebView:** In-App-Browserfenster, das Webseiten innerhalb einer App anzeigt.
- **CTV (Connected TV):** Internetfähige Fernsehgeräte und TV-Plattformen (z. B. Smart-TVs, Streaming-Sticks/Set-Top-Boxen) sowie die darauf betriebenen Streaming-/CTV-Apps.
- **PETs:** Technische Verfahren, die Datenverarbeitung technisch überprüfbar und durchsetzbar machen und die Verarbeitung personenbezogener Daten sowie Datenweitergaben technisch wirksam begrenzen.
- **Targeting (Aussteuerung):** Entscheidung, welche Werbung welcher Zielgruppe oder welchem Kontext angezeigt wird.
- **Profiling (Profilbildung):** Ableitung/Bewertung von Merkmalen oder Interessen einer Person aus Daten, um Verhalten oder Präferenzen einzuschätzen.

- **Attribution (Wirkungsmessung):** Verfahren zur Zuordnung, welche Werbekontakte zu einem Ergebnis beigetragen haben (z. B. Kauf, Registrierung).
- **Minderjährige:** Personen, die das nach Art. 8 DSGVO maßgebliche Mindestalter für eine wirksame Einwilligung noch nicht erreicht haben.
- **Präzise Geodaten**: Standortdaten, die die Bestimmung der aktuellen Position eines Endgeräts innerhalb eines Radius von höchstens 500 Metern (oder genauer) ermöglichen. Hierunter fallen insbesondere GPS-Koordinaten sowie vergleichbare Standortbestimmungsverfahren (z. B. WLAN-/Bluetooth-Beacons, Mobilfunk-Triangulation), soweit sie eine entsprechende Genauigkeit erreichen.

  Standortdaten gelten insbesondere als „präzise", wenn in den gängigen Betriebssystemen die Berechtigung zur „genauen"/„präzisen" Standortfreigabe angefragt wird (z. B. „Precise location"), und nicht lediglich eine vom Betriebssystem bereitgestellte „ungefähre"/„approximate" Standortangabe genutzt wird. Maßgeblich ist hier die vom Betriebssystem definierte Unterscheidung zwischen „precise" und „approximate" sowie die tatsächlich erreichbare Genauigkeit.
- **Betreiber eines digitalen Dienstes:** Marktteilnehmer, der ein digitales Angebot (insbesondere Webseiten, Apps oder vergleichbare digitale Dienste) betreibt oder verantwortet und in seinem Verantwortungs- und Einflussbereich über die Einbindung, Ausgestaltung oder Steuerung von Datenverarbeitungen entscheidet.
- **Endgerät (Endeinrichtung):** Gerät des Endnutzers, das direkt oder indirekt mit einem öffentlichen Kommunikationsnetz verbunden ist und der Sendung, Verarbeitung oder dem Empfang von Informationen dient. Hierzu zählen insbesondere Smartphones, Computer, Tablets, Smart-TVs, Streaming-Sticks/Set-Top-Boxen und vergleichbare vernetzte Geräte.
- **Sensible Daten:** Personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer Person und Daten zum Sexualleben oder zur sexuellen Orientierung einer Person.

Verhaltensregeln

Verantwortliche Praktiken

Die Regeltexte (jeweils Abschnitt „Regel“) sind als Verpflichtungen formuliert und legen fest, was durch Anwender des Kodex umzusetzen ist. Ziele, Abgrenzungen und Erläuterungen beschreiben die Verpflichtungen und den erwarteten Umsetzungsrahmen und unterstützen die einheitliche Anwendung; sie begründen jedoch keine eigenständigen zusätzlichen Pflichten außerhalb des jeweiligen Regeltextes. Ergänzende technische Details, Mess- und Nachweisanforderungen können in einem Annex festgelegt und fortgeschrieben
werden.

Allgemeine Anwendungsbestimmung

Jeder Marktteilnehmer, der den Kodex anwendet, stellt im Rahmen seines jeweiligen Verantwortungs- und Einflussbereichs sicher, dass die nachfolgenden Verhaltensregeln für die von ihm betriebenen oder verantworteten digitalen Angebote und Datenverarbeitungsprozesse (insbesondere Webseiten und Apps) eingehalten werden.

Regel 1 – Proaktive technische Prüfung der in Webseiten und Apps integrierten Ad-Tech Vendoren und der dortigen Datenverarbeitung

Kategorie: Einsatz von Privacy Enhancing Technologies

Ansatz: Technical Compliance Enforcement

Ziel: Aktive technische Kontrolle auf dem Endgerät, ob Nutzereinstellungen (Privatsphäre) und die Vorgaben des Betreibers/Publishers eingehalten werden.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass alle Anbieter von Werbe-Technologien (Vendoren), die auf dem digitalen Dienst direkt eingebunden sind, die von Nutzern vorgenommenen Einstellungen zum Endgerätezugriff und zur Datenverarbeitung befolgen und die Vorgaben des Betreibers für die Einbindung auf diesem digitalen Dienst einhalten.

Der Betreiber überprüft die auf dem Endgerät einsehbaren Zugriffe und Datenverarbeitungen im Hinblick auf die Einhaltung der Nutzereinstellungen sowie seiner Vorgaben **fortlaufend** mit technischen Verfahren, die dem aktuellen Industriestandard entsprechen, und veranlasst bei Abweichungen unverzüglich geeignete Abhilfemaßnahmen.

Erläuterung: Die Prüfung umfasst insbesondere technisch direkt eingebundene Elemente wie Zählpixel/Tracking-Pixel, Tracking-Tags, sowie Skripte (z. B. JavaScript) im Browser und in Apps (z. B. SDKs, In-App-Einbindungen, WebViews) sowie vergleichbare Einbindungsmethoden in weiteren Umfeldern (z. B. Connected TV/CTV). Sie dient dem Nachweis, dass Vendoren weder zusätzliche, nicht freigegebene Zugriffe auslösen noch abweichende Verarbeitungszwecke umsetzen.

Regel 2 – Limitierung der Anzahl der Ad-Tech Vendoren

Kategorie: Selbstlimitierung

Ansatz: Datenstrecken-Kontrolle

Ziel: Sicherstellung eines abgewogenen und aktiv gesteuerten Umfangs der für den digitalen Dienst in der CMP konfigurierten Vendoren und damit des Umfangs der darauf gestützten Datenverarbeitung.

Regel:

Der Betreiber eines digitalen Dienstes verpflichtet sich, die in der Consent-Management-Plattform aktiv konfigurierten Vendoren anhand geeigneter, dokumentierter Auswahl- und

Review-Kriterien (z. B. Märkte, Umfelder [CTV, App, Web] sowie Art der Dienstleistung) auszuwählen und fortlaufend zu überprüfen.

Der Betreiber stellt sicher, dass für den jeweiligen digitalen Dienst auf Grundlage dieser Auswahl- und Review-Kriterien eine dienstweite verbindliche Begrenzung für die Anzahl der aktiv konfigurierten Vendoren festgelegt wird.

Diese Begrenzung ist vom Betreiber regelmäßig zu überprüfen und mit dem Ziel fortzuentwickeln, die Anzahl der aktiv konfigurierten Vendoren auf einen abgewogenen und für den jeweiligen Einsatzfall erforderlichen Umfang zu begrenzen und nach Möglichkeit weiter zu minimieren.

Vendoren, die die festgelegten Auswahl- und Review-Kriterien nicht erfüllen oder für den jeweiligen Einsatzfall nicht erforderlich sind, sind zu deaktivieren oder zu entfernen.

Erläuterung: Die Operationalisierung der Auswahl- und Review-Kriterien kann insbesondere auf Märkte, Umfelder, die Art der Dienstleistung sowie die Erforderlichkeit des jeweiligen Einsatzes gestützt werden. Maßgeblich ist ein nachvollziehbarer, dokumentierter und regelmäßig überprüfter und überprüfbarer Prozess, auf dessen Grundlage der Betreiber für den jeweiligen digitalen Dienst eine angemessene Begrenzung festlegt und die Vendorenstruktur fortlaufend
optimiert.

Regel 3 – Minimierung von Vendoren, die kein standardisiertes Privatsphäre-Framework unterstützen

Kategorie: Selbstlimitierung

Ansatz: Datenstrecken-Kontrolle

Ziel: Verbesserung der Nutzertransparenz und des Nutzervertrauens durch Minimierung von werbewirtschaftlichen Datenverarbeitungen, die nicht (vollständig) über etablierte Privacy-/Consent-Frameworks (z. B. TCF) abgedeckt sind; Standard-Frameworks stärken Transparenz insbesondere durch eine einheitliche Darstellung von Verarbeitungszwecken

und Vendoren, standardisierte Daten- und Zweckkategorien sowie vergleichbare, konsistente Steuerungsmöglichkeiten für Nutzer.

Abgrenzung: Diese Regel bezweckt nicht, einen bestimmten Standard oder ein bestimmtes Framework vorzuschreiben. Sie fördert vielmehr die Vorteile von Standardisierung (Vergleichbarkeit, Verständlichkeit, Kontrollierbarkeit) und lässt funktional gleichwertige Lösungen zu, sofern sie diese Vorteile für Nutzer in gleicher Weise erreichen.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass für werbliche Zwecke solche Vendoren eingesetzt werden, deren Endgerätezugriffe und Datenverarbeitungen vollständig über anerkannte standardisierte Privacy-/Consent-Frameworks abgebildet, gesteuert und transparent gemacht werden können. Vendoren, die für werbewirtschaftliche Datenverarbeitung kein standardisiertes Framework unterstützen, werden auf nachvollziehbar begründete und dokumentierte Ausnahmen reduziert.

Der Betreiber überprüft regelmäßig die Notwendigkeit und Anzahl der eingesetzten Custom-Vendoren und ersetzt, reduziert oder deaktiviert solche Vendoren, sofern die Steuerbarkeit, Transparenz oder Kontrolle nicht in gleichwertiger Weise sichergestellt werden kann.

Erläuterung: Ziel ist die Förderung der Vorteile von Standardisierung (Vergleichbarkeit, Verständlichkeit, Transparenz). Funktional gleichwertige Ansätze sind zulässig, sofern sie die genannten Vorteile für Nutzer in gleicher Weise erreichen.

Regel 4 – Vermeidung ineffizienter Auktionen durch gezielte Steuerung von Nachfragequellen nach Werbeformaten

Kategorie: Selbstlimitierung

Ansatz: Datenstrecken-Kontrolle

Ziel: Minimierung der Datenverarbeitung durch Vermeidung von Auktionsprozessen, die keine verwertbaren Gebote/Nachfrage liefern

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass Auktionsprozesse nur für solche Nachfragequellen ausgelöst werden, bei denen für das jeweilige Werbeformat und das jeweilige Inventar eine konkrete Nachfrage zu erwarten ist, und Nachfragequellen aus Sektionen/Placements entfernt werden, welche keine Nachfrage mehr generieren.

Der Betreiber überprüft (z. B. anhand definierter Schwellenwerte von Gebotsantworten (Bid-Response-Rate) und deren periodischer Auswertung) regelmäßig die Nachfrage der Angebotsplattformen und passt Konfigurationen so an, dass unnötige Auktionen und damit Datenverarbeitungen vermieden werden.

Erläuterung: Maßstab ist die Minimierung unnötiger Datenverarbeitung durch Auktionsprozesse ohne realistischen Ertrag.

Regel 5 – Vermeidung der Monetarisierung von Bot-Traffic

Kategorie: Selbstlimitierung

Ansatz: Inventar-Integrität

Ziel: Sicherstellung eines qualitativ hochwertigen und sicheren Werbeumfeldes durch Erkennung und Ausschluss nicht-menschlichen Traffics

Abgrenzung: Diese Regel adressiert insbesondere automatisierten oder manipulierten Traffic (z. B. Bots, Klick-/Impression-Betrug) im Werbekontext. Sie bezweckt nicht, den Einsatz von durch den Nutzer beauftragten Browser-Agenten („agentic browsing“), die im Auftrag und mit Kenntnis/Willen des Nutzers Schritte auf Webseiten ausführen, zu regeln. Maßgeblich ist, dass automatisierte oder manipulierte Interaktionen, die menschlichen Traffic vortäuschen oder Werbeausspielung/Klicks künstlich erzeugen, nicht als monetarisierbarer Traffic gewertet werden.

Regel:

Der Betreiber eines digitalen Dienstes trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass nicht-menschlicher Traffic nach dem Stand der Technik erkannt und dessen Monetarisierung wirksam minimiert bzw. soweit möglich ausgeschlossen wird.

Der Betreiber setzt hierzu fortlaufend Maßnahmen zur Detektion, Klassifizierung und zum Ausschluss von nicht-menschlichem Traffic ein, die dem aktuellen Stand der Technik und den anerkannten Branchenstandards zur Invalid-Traffic-Erkennung und -Filtration entsprechen. Die Maßnahmen werden regelmäßig auf Wirksamkeit überprüft und optimiert.

Erläuterung: Der Betreiber kann hierfür geeignete Verfahren, Dienstleister oder Kombinationen davon nutzen.

Umsetzungshinweis / Verweis: Die Auslegung von „Stand der Technik“ und „anerkannten Branchenstandards“ kann im technischen Umsetzungshandbuch (Annex) konkretisiert werden, z. B. durch Bezug auf anerkannte Invalid-Traffic-Standards und -Programme sowie kanalbezogene Mess- und Verifikationsstandards (z. B. IAB Tech Lab Open Measurement).

Sofern im jeweiligen Kanal verfügbar, können dabei auch standardisierte Geräte-Authentizitätssignale berücksichtigt werden (z. B. OM SDK Device Attestation zur Reduktion von Device Spoofing im CTV-/App-Kontext). Die Verfügbarkeit solcher Attestation-Funktionen ist plattformspezifisch und hängt von der Unterstützung durch die jeweiligen Geräte-/OS-Ökosysteme ab; Anforderungen und zulässige Evidenzen sind im Annex festzulegen

---

Regel 6 – Anwendung bestehender Standardmechanismen zur Qualitätssicherung der Intermediäre im Supply Path

Kategorie: Selbstlimitierung

Ansatz: Datenstrecken-Kontrolle

Ziel: Minimierung der Datenverarbeitung durch Erkennung und Entfernung redundanter Re-Selling Strecken

Abgrenzung: Diese Regel bezweckt nicht, bestimmte Intermediäre oder Marktteilnehmer zu bevorzugen oder auszuschließen und auch nicht, jede Form des Wiederverkaufs pauschal zu untersagen. Ziel ist allein, redundante Lieferketten und damit verbundene unnötige Datenweitergaben zu reduzieren, soweit diese für den jeweiligen Geschäfts- oder Verarbeitungszweck nicht erforderlich sind.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass Beteiligte in der Lieferkette (Supply Path) fortlaufend anhand anerkannter technischer Industriestandards (insbesondere ads.txt und sellers.json) geprüft werden und redundante Wiederverkaufsprozesse soweit technisch und vertraglich möglich ausgeschlossen und auf ein nachvollziehbar begründetes und dokumentiertes Minimum reduziert werden.

Der Betreiber überprüft regelmäßig die Wiederverkaufs-Struktur (Reseller-Struktur) der angebundenen SSPs und deaktiviert redundante Wiederverkaufs-Strecken durch Entfernung entsprechender Einträge aus seiner ads.txt Datei sowie der Blockierung betroffener SSPs. Verbleibende Redundanzen sind vom Betreiber zu dokumentieren und nachvollziehbar zu erläutern (insbesondere unter Angabe des konkreten geschäftlichen bzw. technischen Grundes sowie der vorgesehenen Maßnahmen und eines Zeitplans zur Reduktion, soweit möglich).

Erläuterung: Ziel ist die Reduktion unnötiger Datenweitergaben entlang redundanter Wiederverkaufs-Ketten (Reselling-Ketten); hierfür ist ein wiederkehrender Prüf- und Bereinigungsprozess erforderlich.

Regel 7 – Keine Weitergabe von präzisen Geodaten an Vendoren und keine Anfrage von Einwilligungen für diese für die Verarbeitung solcher Geodaten

Kategorie: Selbstlimitierung

Ansatz: Verzicht auf als invasiv definierte Verarbeitungen

Ziel: Vermeidung der Bildung weitreichender Bewegungsprofile von Endgeräten und daraus potenziell abgeleiteter sensibler Rückschlüsse durch Dritte, indem die Verarbeitung/Erhebung präziser Geodaten durch in den digitalen Dienst integrierte Vendoren zu werblichen Zwecken ausgeschlossen wird.

Abgrenzung: Diese Regel bezweckt nicht, jegliche Verarbeitung von (präzisen) Geodaten generell auszuschließen. Präzise Standortdaten können für bestimmte legitime Anwendungsfälle erforderlich sein (z. B. standortbezogene Funktionen oder Sicherheits-/Betrugsprävention). Für eine solche Nutzung sind gesonderte Verhaltensregeln zu entwickeln, die so ausgestaltet sind, dass Dritte hieraus keine Bewegungsprofile erstellen und keine Rückschlüsse auf einzelne Personen (z. B. Aufenthaltsorte, Routinen oder sensible Lebensumstände) ableiten können, etwa durch den Einsatz von PETs, Aggregation/Generalisation, Rauschen, On-Device-Verarbeitung oder strikte Zweck- und Zugriffsbeschränkungen. Nicht umfasst ist die Nutzung von aus IP-Adressen abgeleiteten Standortinformationen, sofern diese keine Bestimmung eines konkreten Aufenthaltsortes im Sinne präziser Geodaten ermöglichen.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass präzise Geodaten weder durch in den digitalen Dienst integrierte Vendoren erhoben noch an solche Vendoren weitergegeben werden, soweit dies im technischen und vertraglichen Einflussbereich des Betreibers liegt, und in der CMP keine Einwilligungsabfragen gestellt und keine Konfigurationen vorgenommen werden, die Vendoren eine Rechtsgrundlage (insbesondere eine Einwilligung) zur Verarbeitung präziser Geodaten einräumen oder eine solche Rechtsgrundlage hierfür einholen bzw. gegenüber Vendoren signalisieren.

Der Betreiber unterbindet den Zugriff auf präzise Geodaten durch geeignete technische und organisatorische Maßnahmen und Konfigurationen, die dem Stand der Technik entsprechen, insbesondere durch die CMP-Konfiguration (keine vendorbezogenen Rechtsgrundlagen/Signale für präzise Geodaten), die Konfiguration von App-/SDK-Berechtigungen und Schnittstellen zum Endgeräte-Standort sowie die technische Einschränkung von Tag-/SDK-Einbindungen, die Standortzugriffe auslösen könnten. Der Betreiber überprüft die Wirksamkeit dieser Maßnahmen regelmäßig und nutzt

hierfür insbesondere die in Regel 1 festgelegte fortlaufende technische Prüfung der tatsächlich auf dem Endgerät stattfindenden Zugriffe und Datenverarbeitungen.

Erläuterung: Die praktische Umsetzung erfolgt über die im Regeltext genannten Konfigurationen und Sperren; der fortlaufende Nachweis der Wirksamkeit erfolgt über die Endgeräte-Prüfung nach Regel 1. Unabhängig von Vendor-Anfragen sind Signalisierung und Abfragen zur vendorbezogenen Rechtsgrundlage für präzise Geodaten zu unterbinden.

Regel 8 – Keine Verarbeitung von sensiblen Daten

Kategorie: Selbstlimitierung

Ansatz: Verzicht auf als invasiv definierte Verarbeitungen

Ziel: Sicherstellung eines qualitativ hochwertigen und sicheren Werbeumfeldes durch Ausschluss der Verarbeitung sensibler Daten zu werblichen Zwecken.

Abgrenzung: Politische Meinungen und politische Ausrichtungen gelten im Sinne dieses Kodex als sensible Daten. Diese Regel bezweckt jedoch nicht, politische Werbung als solche zu adressieren oder hierfür Regelungen zu treffen. Gegenstand der Regel ist ausschließlich der Ausschluss der Verarbeitung sensibler Daten im Sinne dieses Kodex zu werblichen Zwecken, insbesondere eben auch solcher Daten oder Merkmale, aus denen politische Meinungen oder politische Ausrichtungen hervorgehen oder aus denen sich nach vernünftigem Maßstab auf solche schließen lässt.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass sensible Daten im Sinne dieses Kodex nicht zu werblichen Zwecken verarbeitet werden.

Er stellt ferner sicher, dass keine gezielte Ableitung oder Nutzung von Merkmalen für werbliche Zwecke erfolgt, die sensible Daten direkt offenbaren oder aus denen sich nach vernünftigem Maßstab auf solche schließen lässt , sofern der Betreiber solche Merkmale selbst erzeugt, bezieht oder nutzt und soweit dies im Verantwortungs- und Einflussbereich des Betreibers für den jeweiligen digitalen Dienst liegt.

Der Betreiber trifft geeignete organisatorische und technische Maßnahmen, um die Verarbeitung sensibler Daten in werblichen Verarbeitungskontexten auszuschließen, und überprüft regelmäßig die Einhaltung.

Erläuterung: Maßgeblich ist der Ausschluss sensibler Daten aus werblichen Verarbeitungskontexten, insbesondere aus Aussteuerung, Profilbildung und Wirkungsmessung.

Regel 9 – Keine gezielte werbliche Ansprache Minderjähriger

Kategorie: Selbstlimitierung

Ansatz: Verzicht auf als invasiv definierte Verarbeitungen

Ziel: Sicherstellung eines qualitativ hochwertigen und sicheren Werbeumfeldes durch den Ausschluss gezielter werblicher Ansprache Minderjähriger.

Abgrenzung: Diese Regel bezweckt nicht, dass Minderjährigen grundsätzlich keine (personalisierte) Werbung mehr angezeigt wird. Unzulässig ist jedoch, Werbung auf Grundlage eines (expliziten oder abgeleiteten) Alters-Profilings einer individuellen Person oder eines Versuchs, die Minderjährigkeit einer bestimmten Person zu identifizieren oder abzuleiten, auszusteuern.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass keine gezielte werbliche Ansprache von Minderjährigen erfolgt und weder ein explizites Altersprofiling noch sonstige Versuche der Identifizierung oder Ableitung der Minderjährigkeit eines individuellen Nutzers zum Zwecke der werblichen Aussteuerung stattfinden.

Der Betreiber implementiert geeignete Maßnahmen, um entsprechende Targeting- und Profiling-Verarbeitungen auszuschließen, und überprüft regelmäßig deren Wirksamkeit.

Erläuterung: Ziel ist ein klarer Ausschluss von „age-based targeting“ und vergleichbaren Segmentierungen, sobald Minderjährigkeit erkannt oder mit hinreichender Sicherheit anzunehmen ist.

Der Stand der Technik entwickelt sich weiter. In den USA führen neue bzw. verschärfte Vorgaben zur Altersabsicherung dazu, dass Plattformen/Betriebssysteme und App Stores altersbezogene Altersbereichs- bzw. Aufsichts-Signale bereitstellen (z. B. Apple „Declared Age Range“ und Google „Play Age Signals“). Sofern solche Signale im jeweiligen Umfeld verfügbar sind und genutzt werden, sind sie datensparsam zu verarbeiten, zweckgebunden zu halten und organisatorisch/technisch so abzusichern, dass sie nicht zur gezielten werblichen Aussteuerung von minderjährigen Personen verwendet werden.

Regel 10 – Durchgängige Anwendung der gleichen Rechtsgrundlage für individuelle werbliche Zwecke

Kategorie: Selbstlimitierung

Ansatz: Konsistente Rechtsgrundlagen

Ziel: Verbesserung der Nutzertransparenz durch Anwendung gleicher Rechtsgrundlagen pro Verwendungszweck und damit klarere und vereinfachte Darstellung.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass für jeden in der CMP ausgewiesenen Verwendungszweck (Purpose) in der CMP einheitlich für alle Vendoren genau eine zulässige Rechtsgrundlage festgelegt ist und diese Festlegung für alle Vendoren technisch durchgesetzt wird, soweit dies durch die eingesetzte Technik/Standards unterstützt wird.

Der Betreiber überprüft regelmäßig die Zweck- und Rechtsgrundlagenkonfiguration in der CMP und beseitigt Abweichungen unverzüglich.

Erläuterung: Die Regel zielt auf Konsistenz und Verständlichkeit; gemischte Rechtsgrundlagen für denselben Zweck (je Vendor unterschiedlich) sollen vermieden werden.

Regel 11 – Zeitfenster für Gültigkeit von Einwilligungen und hinsichtlich erneuter Ansprache

Kategorie: Transparenz & Nutzerkontrolle

Ansatz: (Verantwortungsvolle) Ansprache & Privatsphärekontrolle

Ziel: Sicherstellung transparenter Consent-Praktiken durch angemessene Abstände für erneute Einwilligungsabfragen, die Nutzerentscheidungen respektieren und eine verständliche, konsistente Einwilligungsführung ermöglichen.

Abgrenzung: Diese Regel bezweckt nicht, notwendige erneute Abfragen auszuschließen, wenn sich die Art oder der Umfang der Datenverarbeitung wesentlich ändert oder wenn neue Einwilligungsempfänger (z. B. neu integrierte Vendoren) für einen definierten Zweck eine Rechtsgrundlage benötigen (insbesondere eine Einwilligung). In solchen Fällen ist eine erneute Ansprache zulässig und erforderlich.

Nicht-Umgehung (Klarstellung): Diese Ausnahmen dürfen nicht dazu genutzt werden, den Mindestzeitraum für erneute Abfragen zu umgehen. Insbesondere sind rein formale, geringfügige oder rein organisatorische Änderungen (z. B. Umbenennungen, kosmetische Anpassungen ohne zusätzliche Datenverarbeitung) kein Anlass für eine vorzeitige Wiederansprache.

Regel:

Der Betreiber eines digitalen Dienstes stellt sicher, dass eine Einwilligungsabfrage für einen in der CMP ausgewiesenen Verwendungszweck frühestens nach Ablauf eines Mindestzeitraums erneut gestellt wird, wenn der Nutzer die Erteilung seiner Einwilligung hierfür zuvor verweigert hat, und transparente Regeln zur maximalen Gültigkeit von Einwilligungen sowie zu deren erneuter Bestätigung (Erneuerung/„Refresh“) definiert und in der CMP umgesetzt werden.

Der Mindestzeitraum nach Ablehnung oder Nichterteilung beträgt vier Wochen; die Frist beginnt mit dem Datum der Ablehnung bzw. Nichterteilung der Einwilligung.

Der Betreiber überprüft regelmäßig die Logik für erneute Abfragen und Laufzeit/Erneuerung in der CMP und korrigiert Abweichungen unverzüglich.

Erläuterung: Diese Regel dient der Vermeidung von „Nudging“ durch häufige Wiederansprache; sie trennt Mindestabstand nach „Reject“ und generelle Laufzeit von Einwilligungen.