Länderübergreifende Prüfung des Einsatzes von Tracking-Tools auf Websites von Online-Mediendiensten nach der DS-GVO

Ergänzende Hinweise zur Beantwortung des Fragebogens

Allgemeiner Hinweis

Wird in dem Fragebogen, den Excel-Tabellen oder diesen Hinweisen die Bezeichnung „Dritte“ oder „Drittdienst“ verwendet, ist dies nicht im Sinne von Art. 4 Nr. 10 DSGVO zu verstehen, so dass Auftragsverarbeiter und deren Dienste eingeschlossen sind.

II. Rechtmäßigkeit der Datenverarbeitung gem. Art. 6 Abs. 1 und Art. 9 DS-GVO

Zu II.1

Jedes auf einer Website eingebundene Element oder jeder eingebundene Dienst von Dritten überträgt Daten der Besucher der ursprünglichen aufgerufenen Website an diesen Drittdienstleister. Dies umfasst neben der IP-Adresse auch Nutzungsdaten des Browsers. Ziel der Frage ist es, eine vollständige Übersicht dieser Elemente und Dienste zu erhalten sowie die Form der Einbindung vollständig zu erfassen. Dabei spielt es keine Rolle, ob diese Elemente oder Dienste unmittelbar durch Sie als Betreiber der Website wissentlich technisch implementiert worden sind oder ob derartige Elemente oder Dienste aufgrund des Einsatzes einer Software zur Gestaltung der Website (Software-Suite) Bestandteil des eigenen Angebots geworden sind.

Zu II.2

Ziel der Frage ist es, präzise zu erfassen, welche Daten der Besucher Ihrer Website an Dritte weitergeben und von diesen verarbeitet werden. Neben dem HTTP-Request können dies z. B. eigene Eingaben des Nutzers innerhalb eines von Dritten bereitgestellten interaktiven Inhalts (z. B. interaktive Karte) sein.

Zu II.3

Fingerprinting bezeichnet die aktive oder passive Auswertung von nutzerseitig übermittelten Daten mit dem Ziel eine Wiedererkennbarkeit eines Nutzers oder eines Endgeräts, ohne dass Dateien (z. B. Cookies) auf dem Endgerät des Nutzers abgelegt werden. Die Nutzer können das Fingerprinting zudem nicht durch Voreinstellungen ihres Browsers (z. B. Deaktivierung von Cookie-Einstellungen) generell oder für bestimmte Websites verhindern. Die übermittelten oder serverseitig aktiv angeforderten Daten können mit Hashing-Verfahren zu einem eindeutigen Fingerprint verarbeitet werden und eine dauerhafte Wiedererkennung ermöglichen. Eine Einsatzmöglichkeit von Fingerprinting im First-Party-Kontext ist es, neue Endgeräte zu identifizieren, welche z. B. eine Log-In-Seite benutzen. Weitere Einsatzmöglichkeiten im Third-Party-Kontext sind die Identifizierung und Nachverfolgung von Nutzern sowie die Profilbildung zu diesen. Ziel der Frage ist es herauszufinden, ob der Website-Betreiber selbst oder auf der Website eingebundene Dritte derartige Techniken einsetzen und für welche Zwecke diese genutzt werden.

Zu II.4

Seitens des Website-Betreibers oder eingebundener Dritter besteht die Möglichkeit, eigene Objekte auf dem Endgerät des Nutzers zu speichern und während des Verlaufs eines Besuchs der Website oder auch für längere Zeit zu verarbeiten. Eine eindeutige Zuordnung des Nutzers oder des verwendeten Endgeräts wird damit ermöglicht. Ziel der Frage ist es Erkenntnisse darüber zu erlangen, ob der Website-Betreiber selbst oder auf der Website eingebundene Dritte derartige Techniken einsetzen und auf Basis welcher Rechtsgrundlage diese genutzt werden.

Zu II.5 und II.6

Die Antworten zu der Frage II.5. sollen sich nur auf Datenverarbeitungen beziehen, welche tatsächlich auf eine freiwillige Einwilligung gestützt werden. Dies setzt prinzipiell voraus, dass der Nutzer eine echte Auswahlentscheidung treffen kann, also eine Datenverarbeitung auch ablehnen kann oder eine vergleichbare Alternative zur Auswahl steht. Optionen wie „Verstanden“, „Alles klar“, „Ja und weiter“ oder „Einverstanden“ entsprechen in aller Regel keiner Einwilligung. Derartige Datenverarbeitungen sind dann ggf. unter Frage II.6 zu benennen.

V. Datenschutz-Folgenabschätzung

Zu den Voraussetzungen, wann eine Datenschutz-Folgenabschätzung durchzuführen ist siehe:

- Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf)

- Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf)