

von Rechtsanwalt **Phil Salewski**

Frage des Tages: Datenschutzproblematik bei der Einbindung externer Videos per QR-Code?

Werden Videos auf Webseiten eingebunden, sind unter gewissen Voraussetzungen besondere datenschutzrechtliche Pflichten zu beachten. Hintergrund ist, dass je nach Einbindungsform bei Seitenaufruf oder der Wiedergabe gewisse Nutzerdaten an den Videoanbieter übertragen werden können. Ob und unter welchen Voraussetzungen die Integration von Videos per QR-Code mit dem Datenschutz vereinbar ist, beantworten wir in diesem Beitrag.

I. Datenschutzpflichten abhängig von Form der Video-Einbettung

Soll ein externes Video (etwa von einem Streaming-Dienst wie Youtube) auf einer Internetpräsenz dargestellt werden, kommen grundsätzlich zwei Einbindungsformen in Betracht:

Einerseits ist es möglich, das Video lediglich zu verlinken und Nutzer anzuhalten, sich für die Wiedergabe per Klick auf den Link auf die Webseite des Streaming-Dienstes weiterleiten zu lassen.

Andererseits besteht die Möglichkeit, externe Videos direkt per sogenanntem „Frame“ in die Webseite zu integrieren und so die Wiedergabe direkt auf der Seite selbst zu ermöglichen.

Die Option der bloß externen Verlinkung ist in datenschutzrechtlicher Hinsicht an keinerlei Voraussetzungen gebunden. Datenverarbeitungen, die gegebenenfalls bei Wiedergabe des Videos angestoßen werden, ereignen sich in diesem Fall nämlich ausschließlich auf der externen Seite und mithin außerhalb des Verantwortungsbereich des Seitenbetreibers, der den Link setzt. Wird ein externes Video nur verlinkt, sind weder datenschutzrechtliche Einstellungen noch eine Erwähnung der Verlinkung in der Datenschutzerklärung erforderlich.

Anders sieht es bei der Einbettung von Videos im Wege des „Framing“ aus. Durch die Frame-Integration wird das Video inhaltlicher Bestandteil der Ziel-Webseite und stellt eine permanente Verbindung zu Servern des Streaming-Portals her.

Im Wege der Framing-Einbettung und spätestens im Falle der Wiedergabe im Frame können diverse Nutzerinformationen erhoben und ohne Zutun des Seitenbetreibers an das Streaming-Portal übermittelt werden. Hierfür bedienen sich die gängigen Portale meist Cookies, die auf dem Endgerät des Nutzers gesetzt werden und Informationen auslesen.

Aus diesem Grunde muss bei der Framing-Integration von externen Videos in datenschutzrechtlicher Hinsicht von **datenschutzfreundlichen Grundeinstellungen im Frame über einen rechtskonformen Cookie-Consent bis hin zu einer hinreichenden Klausel in der Datenschutzerklärung** einiges beachtet werden.

Anleitung zum Framing von Youtube-Videos:

Welche Erfordernisse bei der Framing-Einbettung von Youtube-Videos umgesetzt werden müssen, zeigt die IT-Recht Kanzlei [in diesem Beitrag](#) auf.

II. Datenschutzhindernisse für Video-Einbettung per QR-Code?

Eine neue Form, externe Videos zu integrieren, besteht über sogenannte QR-Codes ("Quick-Response-Codes").

Dabei handelt es sich um Matrix-Strichcodes, die mit beliebigen Informationen verknüpft werden und von mobilen Endgeräten ausgelesen werden können, um auf die Informationen zuzugreifen.

Die gängigste Verknüpfung ist die Hinterlegung einer bestimmten Internetadresse im Strichcode so, dass nach dessen Scannen die externe URL geöffnet wird.

Über diese Methode wird per QR-Code auch die Anzeige externer Videos erreicht. Im Code wird die externe Video-URL eingespeist, die sich nach der Erfassung des Codes öffnet.

Was in datenschutzrechtlicher Hinsicht zunächst wie eine weitreichende Informationsverarbeitung anmutet, ist bei näherer Betrachtung grundsätzlich harmlos.

Bei der Hinterlegung eines Video-Links in einem QR-Code handelt es sich technisch nämlich um **nichts anderes als eine Verlinkung** auf eine externe Video-Wiedergabemöglichkeit.

Der QR-Code bzw. dessen Auslesen stoßen selbst keinerlei Datenverarbeitungen an. Vielmehr ereignen sich mögliche Datenverarbeitungen erst nach Weiterleitung auf die verknüpfte Zielseite und mithin außerhalb der Einflussphäre und der Internetpräsenz des Code-Verwenders.

Weil dem Code-Verwender für Datenverarbeitungen auf der mit dem QR-Code verknüpften Zielseite keinerlei datenschutzrechtliche Verantwortung zukommt, ist der Verweis auf externe Videos per QR-Code datenschutzrechtlich ohne Weiteres möglich.

III. Fazit

Bei der Einbettung von QR-Codes, die mit einem Link auf ein externes Video verknüpft sind, handelt es sich in datenschutzrechtlicher Hinsicht um eine einfache Verlinkung auf ein externes Angebot.

Derartige Verlinkungen lösen keine datenschutzrechtlichen Verpflichtungen des Verwenders aus, weil etwaige Datenverarbeitungen sich ausschließlich auf der verlinkten externen Zielseite und mithin außerhalb der datenschutzrechtlichen Verantwortung des Verwenders ereignen.

Weil bei der Einbettung von Videos per QR-Code – anders als beim Framing – die Wiedergabe des Inhalts erst nach Weiterleitung auf die verknüpfte externe Seite möglich ist, treffen datenschutzrechtliche Pflichten im Zusammenhang mit dieser Wiedergabe allein den Betreiber der externen Seite.

Autor:

RA Phil Salewski

Rechtsanwalt