Quick Guide

Mit Bildern und Videos datenschutzkonform kommunizieren

Eine praxisorientierte Einführung

fairpicture

research institute

Wer Bilder und Videos produziert und mit ihnen kommuniziert, sollte sich mit der Datenschutz-Grundverordnung (DSGVO) und weiteren datenschutzrechtlichen Regelungen[1] auseinandersetzen. Der rechtliche Rahmen der Kommunikation mit Bildmaterial wird jedoch von vielen Organisationen oftmals ausgeblendet – mit Konsequenzen für Abgebildete, Bildschaffende und die publizierende Organisation. Bilder und Videos können personenbezogene, sensible oder gar biometrische Daten sein, womit wir uns im Feld des Datenschutzes bewegen. Zudem birgt die Herstellung und Kommunikation mit Bildern diverse Risiken, die auf den ersten Blick nicht unbedingt erkennbar sind. Die Sensibilisierung für rechtlich verpflichtende Risikoanalysen und die in gewissen Fällen zwingend notwendige Einwilligung von Abgebildeten sind wichtige Schritte hin zu einer datenschutzkonformen visuellen Kommunikation.

Dies ist die Zusammenfassung eines Whitepapers, welches das Research Institute Wien mit Unterstützung von Fairpicture erstellt hat. Hier kann das ausführliche Dokument mit mehr Hintergrundinformationen heruntergeladen werden:

https://fairpicture.org/white-paper-data-protection

Um in der Praxis abschätzen zu können, welche rechtlichen Anforderungen wir bei der Erstellung und Veröffentlichung von Fotografien und Videos erfüllen müssen, ist es wichtig, verschiedene Datenkategorien zu unterscheiden.

Bei Bildmaterial handelt es sich um personenbezogene Daten, wenn die abgebildete(n) Person(en) identifiziert werden können. Personenbezogene Daten können unterteilt werden in (1) «normale» personenbezogene Daten und (2) Daten einer besonderen Kategorie/besonders schutzwürdige Daten (im Folgenden «sensible Daten»). Informationen, aus denen die Identität der Person unmittelbar hervorgeht, werden als «primäres Identifikationsmerkmal» bezeichnet. Weitere Informationen, die direkt der identifizierten Person zuordenbar sind, sind ebenso als personenbezogene Daten zu werten. Konkret bedeutet das: Wird der Name einer Person verarbeitet (was bei Fotografien und Videos mit Kontextdaten oft der Fall ist), handelt es sich um ein personenbezogenes Datum. Dann werden sämtliche weiteren Informationen, die dem Bildmaterial zu entnehmen sind, ebenfalls personenbezogen.

Sensible Daten sind dann personenbezogene Daten, wenn daraus etwa die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen. Auch die Verarbeitung von genetischen oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person gehören zu den sensiblen Daten.

Für die Verarbeitung sensibler Daten gelten strengere Anforderungen. So ist eine Verarbeitung auch auf der Grundlage berechtigter Interessen[2] von Medien und Öffentlichkeit nicht zulässig und in der Regel ist eine ausdrückliche Einwilligung erforderlich. Sensible Daten erfordern besondere Sicherheitsmaßnahmen und unter Umständen verpflichtend die Durchführung einer Datenschutz-Folgenabschätzung.

Bei Fotografien und Videos handelt es sich jedoch nicht automatisch um sensible Daten. So ist Bildmaterial, das eine Person mit Brille oder im Rollstuhl zeigt, nicht per se sensibel. Im Lichte der jüngsten Rechtsprechung des Europäischen Gerichtshofes (EuGH) könnte dies jedoch künftig anders zu bewerten und der Anwendungsbereich der sensiblen Daten im Bereich von Bildmaterial früher eröffnet sein. Wenn sich Fotografien und Videos speziell auf sensible Datenkategorien beziehen (wenn sie zum Beispiel Gesundheitsdaten, körperliche oder geistige Einschränkungen, sexuelle Orientierung, ethnische Herkunft, ideologische oder politische Überzeugungen wiedergeben), werden sie in jedem Fall zu sensiblen Daten.

[1] In der Schweiz tritt am 1.9.2023 das revidierte Datenschutzgesetz (DSG) in Kraft. Wir empfehlen, auch in der Schweiz die Standards der DSGVO als Maßstab für die visuelle Kommunikation zu verwenden. Nach dem Schweizer DSG sind Datenverarbeitungen im Ausgangspunkt erlaubt, der scheinbar offene Ansatz wird jedoch durch weitere Vorschriften erheblich eingeschränkt und damit der DSGVO angenähert.

[2] Beispielsweise Ausübung spezieller Grundrechte wie z.B. der Meinungs-, Presse- und Rundfunkfreiheit.

Bildmaterial ist auch nicht automatisch ein biometrisches Datum. Es wird erst dann zu einem solchen, wenn eine spezielle technische Verarbeitung zur Identifizierung einer Person eingesetzt wird wie z. B. bei einem Gesichtserkennungsverfahren.

Aus der DSGVO geht hervor, dass jegliche Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, eine Rechtsgrundlage[3] wie etwa die Einwilligung rechtfertigt die Datenverarbeitung. Für die Verarbeitung von nicht sensiblen personenbezogenen Daten enthält Art 6 DSGVO eine erschöpfende Liste von sechs Rechtsgrundlagen, die eine Datenverarbeitung erlauben:

- die betroffene Person hat ihre Einwilligung zu der Verarbeitung für bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags erforderlich;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich;
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen erforderlich;
- die Verarbeitung ist für die Wahrnehmung einer öffentlichen Aufgabe erforderlich;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen der Verantwortlichen oder einer/eines Dritten erforderlich.

In der DSGVO befinden sich an anderer Stelle[4] jene Rechtsgrundlagen, welche für die rechtmäßige Verarbeitung besonderer Kategorien personenbezogener (bzw. sensibler) Daten erforderlich sind. Da der Gesetzgeber diesen Daten eine höhere Schutzwürdigkeit zuspricht, bestehen erhöhte Anforderungen an die Rechtsgrundlagen für die Verarbeitung besonderer Kategorien personenbezogener Daten.

In diesem Fall sind die speziellen Rechtfertigungstatbestände nach Art 9 DSGVO heranzuziehen. Nach dem Schweizer DSG sind Datenverarbeitungen im Ausgangspunkt erlaubt und erfordern somit grundsätzlich keiner Erlaubnis oder Einwilligung. Das Gesetz hat jedoch strenge Anforderungen an die Verarbeitung personenbezogener Daten, insbesondere darf die Datenverarbeitung nicht die Persönlichkeit der betroffenen Person widerrechtlich verletzen (Art. 30 DSG).

Dabei ist eine Persönlichkeitsverletzung widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (Art. 31 DSG). Dadurch wird der scheinbar offene Ansatz weiterer Vorschriften erheblich eingeschränkt und damit der DSGVO angenähert, die bei jeder Verarbeitung personenbezogener Daten eine Rechtsgrundlage erfordert (Art. 6 DSGVO).

[3] Siehe Art 6, 9 oder 10 DSGVO.

[4] Art 9 Abs 2 DSGVO; vgl. dazu Art 3 lit c DSG – „besonders schützenswerte Personendaten“.

Wann ist die Verarbeitung von sensiblen Daten in der visuellen Kommunikation erlaubt?

Grundsätzlich dürfen Fotografien und Videos nur veröffentlicht werden, wenn sie eine der folgenden Bedingungen erfüllen:

- es existiert eine ausdrückliche Einwilligung der betroffenen Person (Einverständniserklärung);
- es erfolgt eine interne Verarbeitung durch Organisationen ohne Gewinnerzielungsabsicht;
- es werden Bilder verarbeitet, die von den betroffenen Personen selbst offensichtlich öffentlich gemacht wurden, ohne dass diese eine Bearbeitung ausdrücklich untersagt haben;
- die Verarbeitung ist erforderlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte;
- es besteht ein erhebliches öffentliches Interesse;
- die Verarbeitung ist erforderlich für im öffentlichen Interesse liegende Archiv-, Forschungs- oder statistische Zwecke.

Der Umgang mit personenbezogenen und sensiblen Daten bedarf viel Sorgfalt und bewegt sich in einem verbindlichen rechtlichen Rahmen.

Die Wichtigkeit wird umso deutlicher, wenn wir uns vor Augen führen, welche Risiken visuelle Kommunikation mit personenbezogenen und sensiblen Daten für die Bildschaffenden, die Abgebildeten sowie für die kommunizierenden Organisationen selbst birgt. Es ist nicht möglich, alle Risiken auszuschließen, aber die Risikominderung ist rechtlich obligatorisch. Was bedeutet das nun in der Praxis?

Rechtlich verpflichtende Risikoanalyse in der visuellen Kommunikation

Jede Produktion und Verarbeitung von personenbezogenen Daten wie Bildern ist mit Risiken verbunden. Daher ist die Risikobewertung von grundlegender Bedeutung. Alle, die personenbezogenes Bildmaterial herstellen oder verarbeiten, müssen die möglichen Risiken für die Rechte und Freiheiten der abgebildeten Personen in Betracht ziehen. Die DSGVO und das DSG verfolgen dabei einen risikobasierten Ansatz. Verantwortliche[5] sind zur Durchführung einer Risikoanalyse verpflichtet. Die technischen und organisatorischen Maßnahmen müssen die Risiken für die Rechte und Freiheiten von Abgebildeten berücksichtigen. Bestehen hohe Risiken für die Abgebildeten (zum Beispiel Menschen in Konfliktsituationen oder Angehörige vulnerabler Gruppen), sind besondere Maßnahmen wie die Durchführung einer Datenschutz-Folgenabschätzung[6] bzw. eines «Human Rights Impact Assessments» (Grundrechtsassessment) notwendig. Ziel ist es, das Auftreten von Risiken für die Grund- und Menschenrechte der abgebildeten Personen und für die Bildschaffenden zu vermeiden oder auf ein akzeptables Maß zu reduzieren.

Mögliche physische, materielle oder immaterielle Schäden sind:

- drohende Gewalt
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanzieller Verlust
- Schädigung des Ansehens
- unbefugte Aufhebung der Pseudonymisierung
- sonstiger erheblicher wirtschaftlicher oder sozialer Schaden

Der Prozess der Risikobeurteilung lässt sich grundsätzlich in die folgenden methodischen Teilschritte unterteilen:

- Risikoidentifikation

(Beschreibung des Szenarios, Ermittlung beteiligter Akteure und betroffener Personen, Ermittlung der Risikoquelle)

- Risikoanalyse und -bewertung

(Bestimmung der Eintrittswahrscheinlichkeit und Schwere des Schadens ; Bewertung des Risikoszenarios anhand einer Risikomatrix in hoch, normal oder gering)

- Risikobehandlung

(Berücksichtigung bestehender technischer und organisatorischer Maßnahmen der Risikomitigierung; Bestimmung zusätzlicher Abhilfemaßnahmen zur weiteren Minimierung identifizierter Risiken und neuerliche Risikobewertung)

Im Bereich der visuellen Kommunikation gilt es zu beachten, dass sich der Risikokontext von Abgebildeten stark verändern kann (zum Beispiel kann sich die politische Situation in einem Land so verändern, dass bestimmte Gruppen stärker bedroht werden). Wenn sich ein Kontext ändert und abgebildete Menschen infolgedessen Menschenrechtsverletzungen zu befürchten haben, müssen die Verantwortlichen Maßnahmen treffen und beispielsweise bereits publizierte Bilder entfernen, wo dies möglich ist.

[5] “Verantwortliche“ sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, sind sie gemeinsam Verantwortliche und müssen in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO einzuhalten hat (Art 4 Z 7 DSGVO).

[6] Siehe dazu auch das DSG unter Art 22, welches unter bestimmten Umständen ebenfalls verpflichtende Datenschutz-Folgenabschätzungen vorsieht.

[7] Siehe hierzu insbesondere Art 35 Abs 7 sowie ErwGr 76, 77 und 83 DSGVO.

[8] Zum Prozess der Beurteilung wird in ErwGr 76 zudem ausgeführt, dass Eintrittswahrscheinlichkeit und Schwere des Risikos in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden sollten.

Einwilligung und Widerruf der Einwilligung

Datenschutz in der visuellen Kommunikation ist ein Katalysator für Menschenrechte. Oftmals wissen abgebildete Menschen über ihre eigene Gefahrenlage relativ gut Bescheid – ein guter Grund, sie danach zu fragen. Außerdem geht es in visuellen Geschichten um sehr persönliche, manchmal sensible Themen. Die Leitfrage «Wärst du die Person auf diesem Bild, würdest du wollen, dass es veröffentlicht wird?» lässt uns der Thematik nahekommen. Einverständnis hat als wichtiger Pfeiler der DSGVO eine verbindliche rechtliche Grundlage.

Für den Bereich der Bildverarbeitung ist die Einwilligung eine der wichtigsten Rechtsgrundlagen. Sie ist Ausdruck der datenschutzrechtlichen Selbstbestimmung der betroffenen Person, die damit über das «Ob» und «Wie» der Datenverarbeitung entscheidet. Alle Menschen haben das Recht auf ihr eigenes Bild und das Recht auf Privatsphäre. Indem sie die Einwilligung zur Produktion und Verarbeitung ihrer Bilder geben, werden sie zu aktiven Teilnehmenden der Kommunikation und haben Handlungsmacht bezüglich ihrer visuellen Darstellung.

Während das DSG keine ausdrücklichen Vorschriften zur Gestaltung der Einwilligung enthält, macht die DSGVO hier sehr detaillierte Vorgaben.[9] Diese betreffen Grundsätze, die weitgehend auch auf die Schweizer Rechtslage übertragbar sind.

Grundsätze der Einwilligung und deren Widerrufung

Damit Einwilligung rechtlich gültig ist, muss sie freiwillig[10] sein. Sie gilt immer nur für den konkreten Fall und Zweck und erfolgt in Kenntnis der Sachlage. Eine Einwilligung ist eine unmissverständliche Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung. Damit gibt die betroffene Person zu verstehen, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Willensbekundung kann eine Unterschrift sein, aber auch eine unmissverständliche Geste oder die mündliche Zustimmung, die etwa per Video festgehalten ist.

In der DSGVO wird das einfache Widerrufen als notwendig für eine gültige Einwilligung erachtet. Wenn das Widerrufsrecht die Anforderungen der DSGVO nicht erfüllt, steht der Einwilligungsmechanismus der Verantwortlichen also nicht im Einklang mit der DSGVO. Menschen, die eine Einwilligung geben, müssen diese auch zurückziehen können. Sie müssen wissen, wie sie die Verantwortlichen einfach erreichen können und haben das Recht, dass bei Widerruf ihre Daten gelöscht und, wo möglich, auch zurückgezogen werden.

Wenn der Widerrufsprozess nicht gewährleistet werden kann, kommt keine rechtlich gültige Einwilligung zustande!

[9] Siehe dazu auch: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf

[10] Wie die Art-29-Datenschutzgruppe in verschiedenen Stellungnahmen betont hat, kann eine Einwilligung nur dann gültig sein, wenn die betroffene Person eine echte Wahl hat und kein Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher nachteiliger Folgen besteht, sollte sie die Einwilligung nicht erteilen.

Wann ist keine Einwilligung erforderlich?

Es gibt Situationen, in denen die Einholung einer Einwilligung nicht notwendig, besonders umständlich oder sogar unmöglich ist. In Übereinstimmung mit der DSGVO und dem DSG können folgende Ausnahmen festgelegt werden, in denen keine Einwilligung der Abgebildeten notwendig ist:

- die Aufnahme und Veröffentlichung ist Teil eines Vertrags, den die betroffene Person unterschrieben hat;

- die fotografierten/gefilmten Personen sind bereits bei der Aufnahme nicht identifizierbar (anonyme Daten, Datenschutzrecht ist nicht anwendbar);

- Verantwortliche können sich auf eine gesetzliche Grundlage berufen, die die Verarbeitung des Bildmaterials erlaubt bzw. vorschreibt;

- Verantwortliche haben ein berechtigtes Interesse, das die Verarbeitung erforderlich macht, und die Grundrechte der Betroffenen stehen diesem nicht entgegen (Achtung: bei sensiblen Daten und in Bezug auf Kinder ist diese Ausnahme nicht anwendbar!).

In manchen Situationen wird die Einholung einer Einwilligung nicht möglich sein. Wenn sich aus dem Bild oder dem bekannten Kontext keine besonders schutzwürdigen Daten ergeben, ist die Einholung der Einwilligung zumindest nach dem Schweizer Recht in der Regel nicht erforderlich.

Weiterlesen in der ausführlichen Version

Dieses Dokument bietet einen Einstieg in die datenschutzrechtlichen Implikationen der visuellen Kommunikation. Das ausführliche Dokument geht näher auf die angeschnittenen Themen ein. Unter folgendem Link kann das Dokument heruntergeladen werden:

https://fairpicture.org/white-paper-data-protection

Über die Urheber:innen

fairpicture

Fairpicture bietet faire Foto- und Videoaufträge, die ethischen und rechtlichen Kriterien für visuelle Kommunikation entsprechen. Wir entwickeln die Infrastruktur, zum Beispiel die Fairpicture Consent App, um Einwilligungsprozesse rechtskonform und für alle Beteiligten einfach durchzuführen. Außerdem berät Fairpicture Unternehmen zu Themen wie faire und ethische visuelle Kommunikation.

research institute

Das Research Institute in Wien forscht zum Thema Grund- und Menschenrechte in der Digitalisierung an der Schnittstelle von Recht, Technologie und Gesellschaft und berät Organisationen in datenschutzrechtlichen Fragen auch zu visueller Kommunikation. Zahlreiche Erfahrungen in der Erstellung publizierter Datenschutz- Folgenabschätzungen (z.B. zum österreichischen „digitalen Führerschein“ oder zur Stopp-Corona-App des Roten Kreuzes) sowie Human Rights Impact Assessments fließen in ausgewählte Beratungsprojekte ein.