Whitepaper

Mit Bildern und Videos datenschutzkonform kommunizieren

Eine praxisorientierte Einführung

fairpicture research institute

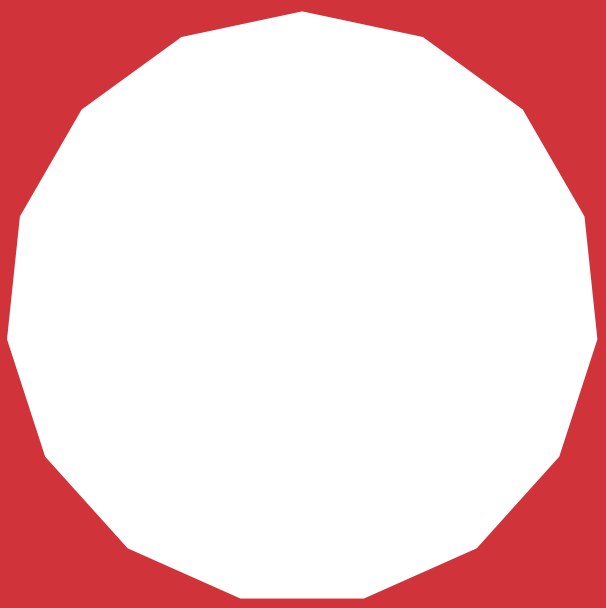
EINLEITUNG

Die Erstellung, Speicherung und Nutzung von Bildern und Videos ist eine verantwortungsvolle Aufgabe. Die Missachtung der Grundrechte von in Bildern und Videos Abgebildeten kann einen nicht zu rechtfertigenden Schaden verursachen. Wer Geschichten von Menschen erzählt, hat verschiedene Anforderungen zu erfüllen. Die Öffentlichkeit hat das Recht, transparent zu erfahren, in welchem Kontext Bilder entstanden und zu verstehen sind und erwartet, dass sie eine wahrheitsgetreue Geschichte erzählen. Auch die Porträtierten haben Rechte und dürfen durch die erzählten Geschichten nicht gefährdet werden. Neben ethischen Grundprinzipen hat dies auch rechtliche Implikationen. Denn nicht die Ausübung, sondern die Einschränkung von Grund- und Menschenrechten wie das Recht auf Datenschutz muss immer gerechtfertigt werden.

Organisationen, die mit Bildern und Videos kommunizieren, haben Pflichten, die über die nach außen hin sichtbare Verwendung von Bildmaterial hinausgehen. Von der Produktion bis hin zur Speicherung der Daten bewegen sie sich in einem rechtlichen Rahmen, dessen Bedingungen vielerorts nicht hinreichend erfüllt werden. Verantwortliche Organisationen oder Bildschaffende, die personenbezogene Daten in Form von Bildmaterial verarbeiten, sind durch die Datenschutz-Grundverordnung (DSGVO) verpflichtet, die Grundrechte von natürlichen Personen zu schützen. Risiken für abgebildete Betroffene müssen zudem minimiert werden. Die DSGVO sowie das revidierte Schweizer DSG, das am 1. September 2023 in Kraft tritt, enthalten Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Sie schützen primär die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf den Schutz personenbezogener Daten. Diese rechtlichen Neuerungen animieren dazu, den Entstehungsprozess und die Verwendung von Bildmaterial aus rechtlicher Perspektive zu beleuchten.

Das vorliegende Whitepaper beschreibt den datenschutzrechtlichen Rahmen visueller Kommunikation in der Schweiz und der EU. Aus dem Verständnis darüber, welche Rechte Abgebildete haben und wie diese eingehalten werden können, leiten sich praxisorientierte Handlungsmöglichkeiten ab. Auf den folgenden Seiten findet sich ein Überblick darüber, wann Bilder personenbezogene und sensible Daten darstellen, in welchen Fällen Einverständniserklärungen verpflichtend sind (und in welchen nicht), und was in diesem Zusammenhang Zweckbindung bedeutet. Außerdem wird ausgeführt, wie die Verantwortlichkeit für die Bilderstellung und Verwendung geregelt ist und wie nach DSGVO verpflichtende Risikoanalysen für potentiell besonders gefährdende Bilder und Videos durchgeführt werden können.

AUTOR:INNEN



Research Institute AG & Co KG
Amundsenstrasse 9
1170 Wien

www.researchinstitute.at

Fairpicture AG
Spitalgasse 28
CH-3011 Bern

www.fairpicture.org

Ing. Dr. iur. Christof Tschohl
ist wissenschaftlicher Leiter und Gesellschafter des Research Institute – Digital Human Rights Center. Er ist Gründungs- und Vorstandsmitglied in der Datenschutz-NGO „noyb“, Co-Arbeitskreisleiter in der Österreichischen Computergesellschaft (OCG Forum Privacy) sowie Mitglied der Fachgruppe Grundrechte der österreichischen Richtervereinigung. In seiner Beraterfunktion ist er außerdem regelmäßig als technischer Sachverständiger der österreichischen Datenschutzbehörde (DSB) im Einsatz.

Dr. iur. Heidi Scheichenbauer
ist als Senior Consultant und Senior Researcher im Research Institute AG & Co KG tätig. Sie hat Rechtswissenschaften an der Universität Wien und der Erasmus Universität Rotterdam mit Schwerpunkt Computer und Recht studiert. Sie ist Mitglied im Verein der behördlichen und betrieblichen Datenschutzbeauftragten (Privacyofficers.at) und Autorin zahlreicher datenschutzrechtlicher Publikationen.

Lisa Seidl, LL.M. (WU)
ist Juristin mit Schwerpunkt Grund- und Menschenrechte, Datenschutz und IP-Recht. Sie wirkt am Research Institute sowohl in der Forschung als auch im Consulting mit und arbeitet dabei regelmäßig an der Schnittstelle von Recht, Technik und Management mit innovativen Ansätzen. In der Datenschutzberatung hat sie einen Schwerpunkt im Bereich von non-profit Organisationen, insbesondere in der fachlichen Betreuung des Network Fair Data (https://researchinstitute.at/network-fair-data/).

Dieses Dokument wurde in Kooperation mit Fairpicture erstellt. Fairpicture ist eine Plattform für faire Foto- und Videoaufträge sowie Stockfotografie/-video, die lokale Bildschaffende aus dem Globalen Süden mit NGOs, Unternehmen, staatlichen Organisationen, Agenturen und Medien aus dem Globalen Norden zusammenbringt. Fairpicture deckt einen Bedarf ab, der immer wichtiger wird: die Beschaffung von fairem, realitätsgetreuem und rückverfolgbarem Foto- und Videomaterial. Durch Consulting, Vorträge und Workshops unterstützt Fairpicture zudem Unternehmen und NGOs in ethischer visueller Kommunikation.

INHALTS-VERZEICHNIS

Bildmaterial als Daten – eine Einordnung

1.1 Bildmaterial als Daten – eine Einordnung

Der Anwendungsbereich des Datenschutzrechts[1] erfordert das Vorliegen von personenbezogenen Daten, die von Verantwortlichen[2] verarbeitet werden. Daraus resultieren Grundpflichten, die von Verantwortlichen einzuhalten sind, sowie Rechte für die von der Verarbeitung betroffenen Personen. Um diese Grundpflichten bzw. Rechte zu erfüllen, müssen technische und organisatorische bzw. vertragliche Maßnahmen getroffen werden. So werden das Grundrecht auf Datenschutz und das Recht auf Privatsphäre nicht verletzt.

1.1.1 Wann liegen personenbezogene Daten vor?

Alle Informationen, die sich auf eine identifizierbare, natürliche Person (im Folgenden „betroffene Person") beziehen, sind vom Begriff „personenbezogene Daten" umfasst. Dazu gehören:

- persönliche Informationen wie Name und Anschrift;
- äußere Merkmale wie Geschlecht, Größe und Gewicht;
- innere Zustände wie Überzeugungen und Meinungen;
- sachliche Informationen wie Vermögens- und Eigentumsverhältnisse und sonstige Beziehungen der Person zu Dritten.

Informationen, aus denen die Identität der Person unmittelbar hervorgeht, werden als „primäres Identifikationsmerkmal" bezeichnet. Weitere Informationen, die infolgedessen direkt der identifizierten Person zuordenbar sind, sind ebenso als personenbezogene Daten zu werten. Wird beispielsweise der Name einer Person verarbeitet (was bei Fotos und Videos mit Kontextdaten oft der Fall ist), handelt es sich um ein personenbezogenes Datum. Folglich sind sämtliche weiteren Informationen, die dem Bildmaterial zu entnehmen sind, personenbezogen.[3]

Empfehlung zum Umgang mit personenbezogenen Daten

Bei der Beurteilung, ob in einem Bild oder Video ein Personenbezug besteht, ist besondere Vorsicht geboten. Dabei ist vor allem zu berücksichtigen, welche Möglichkeiten eines Abgleichs mit anderen Datenbeständen zur Verfügung stehen, die dazu führen, dass Rückschlüsse auf eine bestimmte natürliche Person möglich sind. Für indirekte personenbezogene Daten gelten grundsätzlich dieselben Regeln wie für direkte personenbezogene Daten. Allerdings kann sich bei der Beurteilung der Risiken durchaus ein Unterschied zeigen, wenn sich ein theoretischer Personenbezug nur mit hohem Aufwand herstellen lässt.

1.1.2 Was sind sensible Daten?

Das Datenschutzrecht unterscheidet zwischen normalen personenbezogenen Daten und besonders schutzwürdigen Daten (Daten besonderer Kategorie, häufig „sensible Daten" genannt). Als solche definiert Art 9 Abs 1 DSGVO Daten, aus denen „die rassische [sic!] und ethnische Herkunft, politische

[1] Dieses White Paper ist auf der Grundlage der DSGVO erstellt worden. Der Vergleich zum revidierten Datenschutzgesetz DSG weist bedeutende Unterschiede auf. Dennoch ist die Empfehlung auszusprechen, die Standards der DSGVO möglichst weitgehend als Maßstab zu verwenden. Einen ausdrücklichen rechtlichen Zwang hierzu gibt es für Verantwortliche mit Sitz in der Schweiz nach dem sogenannten „Marktortprinzip" (privatwirtschaftliche Tätigkeit und Ausrichtung auf den Markt der EU). Die DSGVO ist bezüglich der Wahrung der Selbstbestimmung strenger als das Schweizer DSG, wodurch im Fall der visuellen Kommunikation auch ethischen Ansprüchen Rechnung getragen wird.

[2] Verantwortlicher im Sinne der DSGVO ist nach Art. 4 Ziffer 7 DSGVO derjenige, der über die Mittel und den Zweck der Verarbeitungen entscheidet.

[3] Die Literatur und unionsrechtliche Judikatur setzen am „relativen Personenbezug oder an der relativen Theorie" an, wonach für die Qualifikation einer Einzelangabe als personenbezogenes Datum die Kenntnisse und Mittel der datenverarbeitenden Stelle ausschlaggebend sind. Danach richtet sich letztendlich die Identifizierbarkeit. Es sind alle (rechtlich zulässigen) Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden. Sofern Verantwortliche (auch über die den Verantwortlichen zurechenbaren (Sub-)Auftragsverarbeiter) durch relevantes Zusatzwissen Einzelangaben einer Person direkt zuordnen können, ist die Identifizierbarkeit zu bejahen, wodurch diese Einzelangaben für die datenverarbeitende Stelle als personenbezogene Daten zu qualifizieren sind.

Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschafts-zugehörigkeit“ hervorgehen, sowie die „genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“.[4] Die Verarbeitung solcher Daten ist untersagt. In Abs 2 werden die Ausnahmen vom Verarbeitungsverbot geregelt.

Nach jüngster Rechtsprechung des EuGH[5] sind auch Daten von dieser Kategorie umfasst, die nicht ihrem Wesen nach sensibel sind, sondern durch Rückschlüsse auf diese Daten hervorgehen. Im Beispiel des genannten Falles geht die sexuelle Orientierung erst durch die gedankliche Kombination hervor, die die Erwähnung der Namen der Lebenspartner:innen ermöglicht. Hierbei gehen indirekt sensible Daten hervor. Dass diese weite Auslegung für alle „besonderen Kategorien personenbezogener Daten“ gilt, ist anzunehmen.

Grundsatz des Rechts auf Datenschutz

Jede Verarbeitung von personenbezogenen Daten ist nach der DSGVO grundsätzlich verboten, es sei denn, es gibt eine Ausnahme von diesem Verbot. Im Fall von sensiblen Daten sind diese Ausnahmegründe eingeschränkt, weshalb oftmals nur die freiwillige Einwilligung eine Ausnahme bilden kann.

1.1.3 Wann Bilder besonders schützenswerte Daten sind

Bildmaterial von natürlichen Personen beinhaltet häufig Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Die Abgebildeten sind dann betroffene Personen im Sinne der DSGVO. Die Bedingung für einen „Personenbezug“ bei Abbildungen von Personen ist, dass die abgebildeten Personen erkennbar sind. Auch Bilder von Menschen beim Betreten oder Verlassen von öffentlichen Bereichen, von denen der Name häufig nicht bekannt ist, werden als identifizierbare Bilder mit Personenbezug qualifiziert, da eine nachträgliche Identifizierung möglich ist. Nicht personenbezogen sind Daten dann, wenn Personen nicht erkennbar sind. Es muss jedoch berücksichtigt werden, dass aufgrund von Kontextinformationen auch die Möglichkeit bestehen kann, vermeintlich unkenntlich abgebildete Personen zu identifizieren. Auch dann liegt ein Personenbezug vor. Das kann etwa der Fall sein, wenn bestimmte Orte oder Räumlichkeiten in Verbindung mit weiteren verfügbaren Informationen (zum Beispiel Schriftzüge, Adressen, aber auch etwa öffentlich zugängliche Inhalte auf Sozialen Medien) einer bestimmten Person zugeordnet werden können.

Bildmaterial wird im europäischen Recht nicht automatisch als den besonderen Datenkategorien bzw. sensiblen Daten zugehörig betrachtet. Bislang wurde vom Europäischen Datenschutzausschuss (EDSA) ausgesprochen,[6] dass Videoaufnahmen, die eine betroffene Person mit Brille oder im Rollstuhl zeigen, nicht per se als besondere Kategorien personenbezogener Daten gelten. Man könnte anhand von Bildmaterial etwa Rückschlüsse auf den Gesundheitszustand oder die ethnische Herkunft von natürlichen Personen ziehen oder Bildmaterial als (sensibles) biometrisches Datum ansehen. Auch wenn das jedoch nicht die Absicht der Verantwortlichen ist, kann dies entlang der jüngsten Rechtsprechung des EuGH anders zu bewerten sein. Entsprechendes Bildmaterial kann aber jedenfalls dann besondere Kategorien personenbezogener Daten offenbaren, wenn der Zweck der Verarbeitung die Ableitung von sensiblen Daten darstellt.

[4] Besonders schützenswerte Daten unterliegen besonderen Anforderungen: So ist zum Beispiel die Verarbeitung aufgrund berechtigter Interessen nicht zulässig und es ist häufig eine ausdrückliche Einwilligung erforderlich. Zudem kann das Vorliegen von sensiblen Daten das Ergreifen von besonderen Sicherheitsmaßnahmen erfordern oder die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung nach sich ziehen.

[5] EuGH, 1.8.2022, C-184/20.

[6] EuGH, 1.8.2022, C-184/20.

Auch die Verwendung biometrischer Daten (Bilder, die „zur eindeutigen Identifizierung einer natürlichen Person“ verarbeitet werden)[7] birgt erhöhte Risiken für die Rechte betroffener Personen.

Nach Art 4 Z 14 und 15 DSGVO liegen biometrische Daten dann vor, wenn folgende drei Kriterien erfüllt werden:

- es liegen Daten über physische, physiologische oder verhaltensbezogene Eigenschaften einer natürlichen Person vor;
- es muss sich um „mit speziellen technischen Verfahren gewonnene“ Daten handeln;
- die Daten müssen zur eindeutigen Identifizierung einer natürlichen Person verwendet werden können.

Damit Daten als biometrische Daten im Sinne der DSGVO eingestuft werden können, muss ihre Verarbeitung nach Ansicht des Europäischen Datenausschusses EDSA eine Messung solcher Merkmale implizieren.

1.1.4 Technische Daten und Metadaten als personenbezogene Daten

Nach unserem Ansatz wird durch Metadaten (z.B. Geo-Daten, Namen, Alter, ausführliche Beschreibung des Kontextes) eine Zweckbindung im Zusammenhang mit der Bildverwendung sichergestellt. Detaillierte Bildunterschriften minimieren das Risiko für den Bildautor und das Reputationsrisiko, das sich aus einer unangemessenen Verwendung von Bildern ergibt.
Neben dem Bildmaterial selbst ist zu beachten, dass auch Daten aus dem technischen Verarbeitungsprozess sowie Metadaten zu den personenbezogenen Daten zählen können. Gerade technische Daten sind nicht selten als personenbezogen zu qualifizieren, wenngleich es sich typischerweise um (hoch) pseudonymisierte, aber eben nicht vollständig anonymisierte Daten handelt.[8]

Empfehlung zur Kategorisierung von Bildmaterial

Personenbezogene Daten können in normale personenbezogene Daten und in Daten besonderer Datenkategorie unterteilt werden. Für die Verarbeitung sensibler Daten gelten strengere Anforderungen.

Ein Bild, das zum Beispiel eine betroffene Person mit Brille oder im Rollstuhl zeigt, kann den besonderen Datenkategorien zugehörig betrachtet werden, da auch indirekt abgeleitete sensible Daten als solche zu werten sind (Gesundheitsdaten, sexuelle Orientierung, weltanschauliche oder politische Überzeugung, rassische [sic!] oder ethnische Herkunft).

Bildmaterial wird erst dann zum biometrischen Datum, wenn eine spezielle technische Verarbeitung erfolgt, die der Identifizierung einer Person dient – etwa über Gesichtserkennungsverfahren.

1.2 Wer ist für den Datenschutz verantwortlich?

Datenschutzrechtliche Pflichten und Rechte der Betroffenen knüpfen nach der DSGVO großteils an die Verantwortlichkeit an. „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 entscheidet. Sofern zwei oder mehr Verantwortliche gemeinsam

[7] Bei Bildmaterial einer Person handelt es sich nicht um biometrische Daten, wenn es nicht speziell technisch verarbeitet wurde, um zur Identifizierung oder Authentifizierung einer Person beizutragen.

[8] Das liegt daran, dass solche Daten in der Regel in einer hoch strukturierten Form verarbeitet werden und damit auch durch einen komplexeren Abgleich mit anderen (z.B. bereits öffentlichen) Daten zugänglich sind, der zu einer Identifizierung der Person führen kann. Nach der Leitentscheidung des EuGH sind z.B. „dynamische IP-Adressen einer natürlichen Person für den Anbieter als personenbezogene Daten gem. Art 4 Z 1 DSGVO zu beurteilen, sofern der Anbieter über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen (...) bestimmen zu lassen.“ (EuGH 19. 10. 2016, C-582/14, Breyer/BRD.)

[9] EuGH, 1.8.2022, C-184/20.

die Zwecke der und die Mittel zur Verarbeitung festlegen, sind sie gemeinsam Verantwortliche und müssen in einer Vereinbarung in transparenter Form festlegen, wer welche Verpflichtung gemäß der DSGVO einzuhalten hat.[9]

Von den „Verantwortlichen“ müssen „Auftragsverarbeiter:innen“ unterschieden werden: Laut DSGVO sind „Auftragsverarbeiter:innen“ natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag der Verantwortlichen verarbeiten.[10]

Liegt eine Auftragsverarbeitung vor, ist nach der DSGVO zwingend eine Auftragsverarbeitungsvereinbarung (AVV) abzuschliessen.[11] Auftraggeber:innen sind für die Einhaltung der gesetzlichen Datenschutzvorschriften allein verantwortlich. Dementsprechend sind sie auch verpflichtet, Auftragnehmer:innen sorgfältig auszuwählen und haben sich von der Einhaltung der bei den Auftragnehmer:innen getroffenen technischen und organisatorischen Maßnahmen nach Art 32 DSGVO zum Schutz der personenbezogenen Daten zu überzeugen („hinreichende Garantien“).

Auftragnehmer:innen müssen sicherstellen, dass die Datenverarbeitung nach den durch Auftraggeber:innen erteilten Weisungen erfolgt.

Wenn mehrere Stellen tätig werden/agieren, ist die Rollenverteilung zu klären. Zu definieren ist, wer die Mittel und Zwecke der Datenverarbeitung (die Beauftragung und die Verarbeitung des Bildmaterials) verantwortet. Wenn verschiedene Stellen über Mittel und Zwecke zusammen entscheiden, ist eine gemeinsame Verantwortlichkeit anzunehmen. Wenn nur im Auftrag einer Stelle Daten (d.h. Bilder) verarbeitet werden, ist von einer Auftragsverarbeitung auszugehen.

Empfehlung zur Berücksichtigung von Metadaten

Bildschaffende sollten klare Anweisungen erhalten, welche Metadaten erwartet werden, die jedem Bild (oder jeder Gruppe von Bildern) beizufügen sind. Inhaltliche Metadaten sollen die fünf W-Fragen beantworten: Was ist zu sehen? Wer ist zu sehen? Wo, wann und warum wurde das Bildmaterial erstellt? Technische Vorkehrungen sollen verhindern, dass Metadaten nachträglich unautorisiert abgeändert werden.
Zu bedenken gilt hier allerdings, dass Transparenz durch ausführlichere und öffentlich zugängliche Informationen in gewissen Risikokontexten (z.B. Reportage über kurdische Widerstandskämpfer:innen) auch besondere Risiken produzieren können. Fairpicture arbeitet aktuell an Ansätzen, wie Kontext-informationen kryptographisch geschützt werden können (inkl. der Transparenzfragen); ein interessantes Beispiel für diesen Mechanismus ist c2pa, das technisch in eine ähnliche Richtung geht: https://c2pa.org/.

Jedes Bild sollte mit den folgenden zehn Schlüssel-Metadaten für alle Abzubildenden/Abgebildeten (die deutlich sichtbar sind) ergänzt werden:

- vollständiger Name
- Pseudonym (falls zutreffend)
- Geburtsdatum
- Überschrift
- Datum, an dem die Geschichte gesammelt wurde
- geografischer Standort
- Beschreibung der Programmarbeit
- Name/Nummer des Projekts
- Partnerorganisation
- Bildgestalter/Agentur

[9] Art 4 Z 7 DSGVO.

[10] Art 4 Z 8 DSGVO.

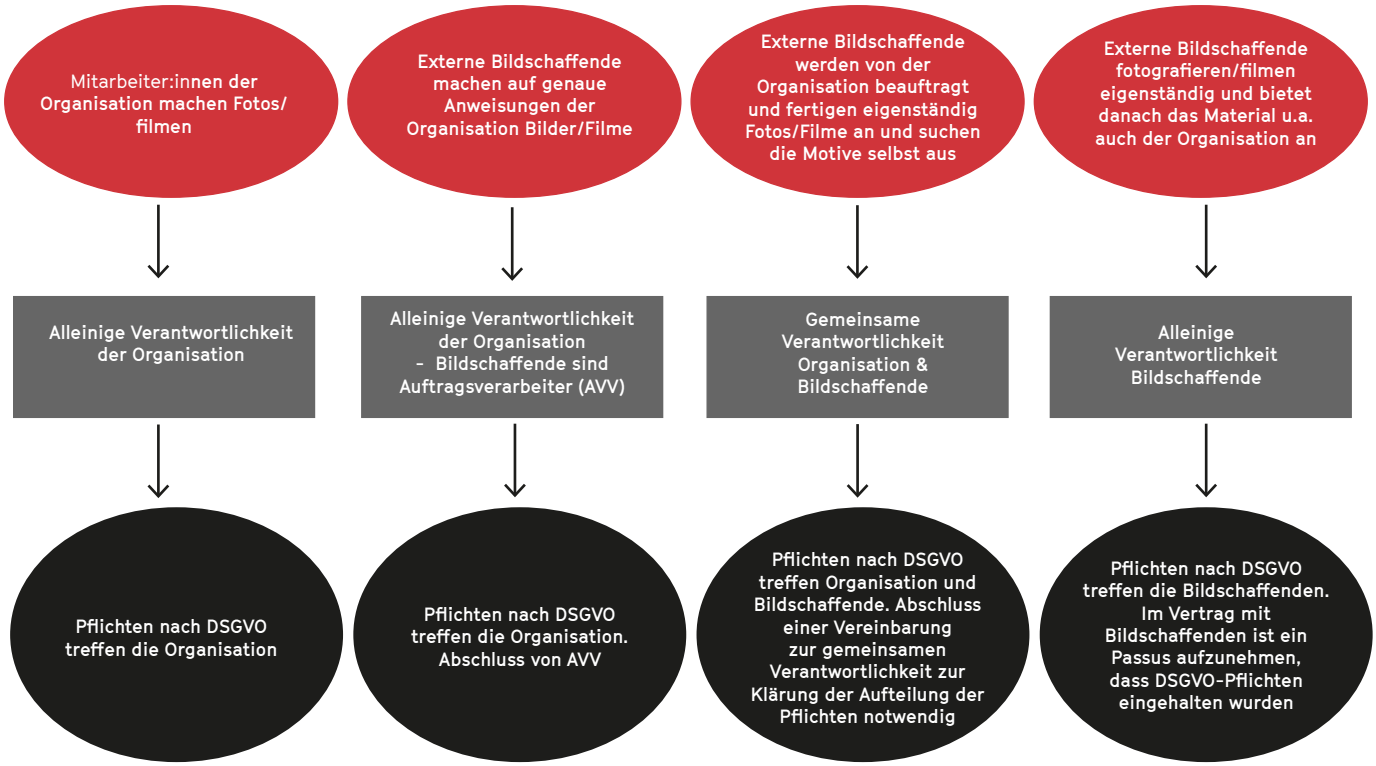
[11] Das DSG kennt hingegen keine ausdrückliche Verpflichtung, eine solche Auftragsverarbeitungsvereinbarung abzuschließen.

Wenn gemeinsam entschieden wird, wie die Daten abgelegt werden, ist bei der Beurteilung Vorsicht geboten: Hat der/die Verantwortliche, der/die über die Zwecke allein entscheidet, nur bestimmte Details in der technischen Umsetzung an einen Erfüllungsgehilfen delegiert, liegt nur eine Auftragsverarbeitung vor. Wenn aber tatsächlich eine gemeinsame Entscheidung über die Mittel (also über das „Wie“) erforderlich ist, dann liegt eine gemeinsame Verantwortung im Sinne des Art 26 DSGVO vor.

Bildschaffende können als Auftragsverarbeiter:innen betrachtet werden, wenn sie im Auftrag und auf Weisung eines/einer Auftraggeber:in handeln. Dies erfordert den Abschluss einer Auftragsverarbeitungsvereinbarung Hier ist jedoch nicht abschließend geklärt, wie stark die Weisungsgebundenheit der Bildschaffenden sein muss, um diese anzunehmen. Bildschaffende können auch so selbständig und weisungsfrei handeln, dass kein Fall der Auftragsverarbeitung vorliegt und sie somit eigenständig Verantwortliche sind. Dies ist dann der Fall, wenn Bildschaffende ihre Motive eigenständig suchen und lediglich die Endergebnisse an Auftraggeber:innen verkaufen.

Bei offenen Briefings[12] ist eher von einer gemeinsamen Verantwortung auszugehen. Sofern Bildschaffende bei der Erfüllung von Aufträgen weitestgehend eigenständig handeln, kann mit Auftraggeber:innen eine Konstellation der „gemeinsamen Verantwortlichkeit“ nach Art 26 DSGVO vorliegen. So entscheiden die Verantwortlichen gemeinsam über Zweck und Mittel der Verarbeitung. Eine gemeinsame Verantwortlichkeit hätte zur Folge, dass Bildschaffende die weiter oben beschriebenen Pflichten der DSGVO grundsätzlich selbst erfüllen müssen. Auch hier ist eine Vereinbarung zu treffen, in der festgelegt wird, wer etwa die Informationspflichten erfüllt. Nach Art 26 Abs 2 DSGVO muss die abzuschließende Vereinbarung aber jedenfalls die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen gebührend widerspiegeln.

Bildschaffende können auch Mitarbeiter:innen der Verantwortlichen sein. In einem solchen Fall sind die Mitarbeiter:innen ebenfalls zur Vertraulichkeit zu verpflichten.[13]



[12] Etwa wenn Bildschaffende beauftragt werden, ein Projekt zu besuchen und zu dokumentieren, aber nicht geregelt ist, wie diese Dokumentation aussehen soll.

[13] Art 29 DSGVO.

1.3 Wie wird Datenschutz sichergestellt?

Die folgenden Grundsätze stellen die „Grundpflichten“ nach der DSGVO dar, deren Einhaltung von den Verantwortlichen gewährleistet werden muss:

- Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz[14]: Für die Verarbeitung personenbezogener Daten gilt laut DSGVO ein sog. Verbot mit Erlaubnisvorbehalt. Es muss also stets ein „Erlaubnistatbestand“ bestehen, damit personenbezogene Daten verarbeitet werden dürfen. 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.[15] Datenverarbeitung nach Treu und Glauben bzw. transparente Datenverarbeitung setzen voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß sowie umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden.

- Zweckbindung: Die Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden. Daten dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.[16]

- Datenminimierung: Die Daten dürfen nur dem Zweck angemessen verarbeitet werden und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Es sollten daher nur so wenige personenbezogene Daten verarbeitet werden, wie für den Zweck erforderlich. Diese Daten sind zudem zu löschen, wenn sie für die Zweckerfüllung nicht mehr erforderlich sind.[17]

- Richtigkeit: Die Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Wenn neue Zwecke angestrebt werden, müssen entsprechend auch erneut die Abgebildeten informiert werden und die Frage nach den Rechtsgrundlagen neuerlich aufgerollt werden.[18]

- Speicherbegrenzung: Die Speicherdauer ist auf das unbedingt erforderliche Mindestmaß zu beschränken.[19]

- Integrität und Vertraulichkeit: Die Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich ihren Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Dies wird durch geeignete technische und organisatorische Maßnahmen sichergestellt.[20]

Auch wenn die Terminologie nicht exakt dieselbe ist und manche Grundsätze nicht ausdrücklich formuliert sind, finden sich auch im Schweizer DSG[21] vergleichbare Ansätze. Das systematische Verständnis der Grundsätze ist im Rahmen der beiden Regularien nicht grundlegend verschieden und es wird daher dringend empfohlen, sich an den hier wiedergegebenen Begriffen der DSGVO zu orientieren. Diese sind auch nach der Schweizer Rechtslage zumindest nachvollziehbar und verständlich.

1.4 Die Einwilligung als Rechtsgrundlage nach der DSGVO

Aus der DSGVO geht hervor, dass jegliche Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist, es sei denn, eine Rechtsgrundlage des Art 6, 9 oder 10 DSGVO (wie zum Beispiel die Einwilligung) rechtfertigt

[14] Art 5 Abs 1 lit a DSGVO.

[15] Das Schweizer DSG erfordert grundsätzlich keine Erlaubnis oder Einwilligung. Das Gesetz hat jedoch strenge Anforderungen an die Verarbeitung personenbezogener Daten. Ein Rechtfertigungsgrund ist dann nötig, wenn entweder die Bearbeitungsgrundsätze (Art. 6 und 8 revDSG) nicht eingehalten werden, die betroffene Person der Bearbeitung widersprochen hat (Art. 30 Abs. 2 Bst. b revDSG) oder einem Dritten besonders schützenswerte Personendaten mitgeteilt werden sollen (Art. 30 Abs. 2 Bst. c revDSG). Dadurch wird der scheinbar offene Ansatz weiterer Vorschriften erheblich eingeschränkt und damit der DSGVO angenähert. Vgl. dazu Rosenthal, Das neue Datenschutzgesetz, Jusletter 2020.

[16] Art 5 Abs 1 lit b DSGVO.

[17] Art 5 Abs 1 lit c DSGVO.

[18] Art 5 Abs 1 lit d DSGVO.

[19] Art 5 Abs 1 lit e DSGVO.

[20] Art 5 Abs 1 lit f DSGVO.

die betreffende Datenverarbeitung. Für die Verarbeitung von nicht sensiblen personenbezogenen Daten enthält die 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[22] jene Rechtsgrundlagen, welche für die rechtmäßige Verarbeitung besonderer Kategorien personenbezogener (sensibler) Daten[23] erforderlich sind. Da der Gesetzgeber diesen Daten eine höhere Schutzwürdigkeit zuspricht, bestehen erhöhte Anforderungen an die Verarbeitung besonderer Kategorien personenbezogener Daten. In diesem Fall sind die speziellen Rechtfertigungstatbestände nach Art 9 DSGVO heranzuziehen. Die in Betracht kommenden Erlaubnistatbestände für die Verarbeitung von sensiblen Daten in der visuellen Kommunikation sind:

- ausdrückliche Einwilligung der betroffenen Person;
- interne Verarbeitung durch Organisationen ohne Gewinnerzielungsabsicht;
- die Verarbeitung von offensichtlich öffentlich gemachten Daten durch die betroffene Person selbst, wenn diese gleichzeitig eine Bearbeitung nicht ausdrücklich untersagt hat;

HINWEIS

Der für die Praxis der visuellen Kommunikation wohl bedeutendste Unterschied zwischen der DSGVO und der DSG liegt in den Anforderungen an die Rechtsgrundlage der Verarbeitung, insbesondere an die Einwilligung. Nach dem Schweizer DSG ist für die Verarbeitung von Personendaten grundsätzlich zwar kein Rechtfertigungsgrund (also auch keine Einwilligung) notwendig. Ein Rechtfertigungsgrund ist jedoch dann nötig, wenn die Bearbeitungsgrundsätze (Art. 6 und 8 DSG) nicht eingehalten werden, Betroffene der Bearbeitung widersprochen haben (Art. 30 Abs. 2 Bst. b DSG) oder einem Dritten besonders schützenswerte Personendaten mitgeteilt werden sollen (Art. 30 Abs. 2 Bst. c DSG).[24]
Das ist im Kontext visueller Kommunikation beispielsweise dann erfüllt, wenn die Bilddarstellung potentiell die Würde der abgebildeten (und identifizierbaren, also vor allem erkennbaren) Menschen berührt oder wenn gerade durch die Abbildung eine Gefahr für die Sicherheit, die Freiheit oder für Leib und Leben der betroffenen Personen entsteht. Dazu ist eine Risikobeurteilung erforderlich.

- die Erforderlichkeit der Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte;
- aus Gründen eines erheblichen öffentlichen Interesses;

[21] Siehe Art 6 DSG; Jedoch ist zu berücksichtigen, dass ab 1.9.2023 das Schweizer Datenschutzrecht novelliert wird: siehe dazu: https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/datenschutzstaerkung/vdsg/vo.pdf.

[22] Art 9 Abs 2 DSGVO; vgl. dazu Art 3 lit c DSG – „besonders schützenswerte Personendaten". Gem. Art 9 Abs 1, Art 4 Z 13 - 15 DSGVO.

[23] Sensible Daten/besondere Datenkategorien sind personenbezogene Daten, aus denen rassische [sic!] und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

- die Erforderlichkeit für im öffentlichen Interesse liegende Archiv-, Forschungs- oder statistische Zwecke.

1.4.1 Einwilligung als Rechtsgrundlage und Erfüllung der Informationspflichten

Für den Bereich der Bildverarbeitung ist die Einwilligung eine der wichtigsten Rechtsgrundlagen bei der Verarbeitung personenbezogener Daten. Die Einwilligung ist Ausdruck der datenschutzrechtlichen Selbstbestimmung der betroffenen (also abgebildeten) Person, die damit über das „Ob" und „Wie" der Datenverarbeitung entscheidet.

1.4.2 Anforderungen an eine gültige Einwilligung

Während das DSG keine ausdrücklichen Vorschriften zur Gestaltung der Einwilligung enthält, trifft die DSGVO hier sehr detaillierte Vorgaben, die möglicherweise künftig durch die Rechtsprechung auch auf die Schweizer Rechtslage übertragbaren werden. Insbesondere geht es dabei um Wahrung der Freiwilligkeit und Transparenz als Voraussetzungen für eine wirksame Einwilligung.

Art 4 Z 11 und 7 DSGVO legen die Bedingungen für die Einwilligung einer betroffenen Person fest. Sie muss folgende Punkte erfüllen:

- freiwillig;
- für den bestimmten Fall;
- in informierter Weise und
- unmissverständlich abgegebene

Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Um freiwillig zu sein, muss ein Ungleichgewicht der Macht vermieden werden. 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 (z. B. erhebliche Zusatzkosten) besteht, sollte sie die Einwilligung nicht erteilen. In Fällen, in denen Zwang oder Druck ausgeübt wird oder keine Möglichkeit zur Ausübung des freien Willens besteht, ist eine Einwilligung nicht frei.

Damit eine Einwilligung in informierter Weise erfolgt und gültig ist, muss die abzubildende Person über mindestens folgende Informationen vor der Anfertigung von Bildmaterial verfügen:

- die Identität der Verantwortlichen;
- der Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird;
- die (Art der) Daten, die erhoben und verwendet werden;
- das Bestehen des Rechts, die Einwilligung zu widerrufen[26];
- Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung gemäß Art 22 Abs 2 Buchstabe c DSGVO[27], wenn eine solche vorliegt, und
- Angaben zu möglichen Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art 46 DSGVO.

[24] Rosenthal, Das neue Datenschutzgesetz, Jusletter 2020.

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

[26] Hinweis: Dies gilt zwar nicht nach Schweizer Recht, aber zwingend nach Art 7 DSGVO. Die Einwilligung muss genauso leicht widerrufbar sein, wie sie erteilt worden ist. Weitere Vorgaben zum Prozess des Widerrufs bestehen nicht.

[27] Vgl. dazu Art. 21 Abs. 3 lit b DSG.

Eine gültige Einwilligung „in informierter Weise“ kann auch dann vorliegen, wenn nicht sämtliche Elemente der Datenschutzinformationen beim Einholen der Einwilligung unmittelbar genannt werden. Die Liste der verpflichtenden Informationen nach Art 13 und 14 DSGVO ist umfangreicher als jene Informationen, die im unmittelbaren Einwilligungstext ersichtlich sein müssen. Die weitergehenden Informationen dürfen zum Beispiel in einem zusätzlichen Text stehen, der unter einem Online-Link oder auf einem Beiblatt physisch verfügbar ist. Nicht jede Verletzung der Informationspflicht berührt automatisch die Gültigkeit der Einwilligung.

Unwirksam ist die Einwilligung allerdings dann, wenn die Informationen gar nicht vorhanden sind oder so lückenhaft, dass für Betroffene weder Zwecke noch Empfänger transparent sind. In diesem Fall ist der Transparenzgrundsatz verletzt und die Einwilligung deshalb unwirksam.

1.4.3 Welche Form können Einverständniserklärungen haben?

Die DSGVO schreibt ebenso wenig wie das DSG vor, in welcher Form die Informationen bereitzustellen sind, um das Erfordernis der Einwilligung in informierter Weise zu erfüllen. Gültige Informationen können also auf verschiedene Weise vorgelegt werden, beispielsweise als schriftliche oder mündliche Erklärungen oder als Audio- oder Videonachrichten. Die Verantwortlichen sollten die Einwilligungsmechanismen so konzipieren, dass sie für die betroffenen Personen verständlich sind. Eine informierte Einwilligung soll außerdem in der Sprache der Person erfolgen.

Die DSGVO macht – anders als das hierzu deutlich mildere DSG – deutlich, dass eine Einwilligung, eine Erklärung oder eine eindeutige bestätigende Handlung seitens der betroffenen Person erforderlich ist. Die Einwilligung muss folglich stets durch eine aktive Handlung oder Erklärung erteilt werden und kann nicht durch einen unterlassenen Widerspruch erteilt werden.

Die Einwilligung zur Verarbeitung personenbezogener Daten muss nicht zwingend schriftlich erfolgen. Eine Einwilligung kann daher durch eine schriftliche oder aber durch eine (aufgezeichnete) mündliche Erklärung, die auch elektronisch erfolgen kann, eingeholt werden. Die Verantwortlichen sollten die Einwilligungsmechanismen so konzipieren, dass sie für die betroffenen Personen verständlich sind. Die Verantwortlichen müssen Unklarheiten vermeiden und sicherstellen, dass die Handlung, mit der die Einwilligung erteilt wird, von anderen Handlungen unterschieden werden kann. Das heißt, eine Geste oder ein Verhalten darf im konkreten Zusammenhang keinen Zweifel daran lassen, dass damit eben gerade eine Einwilligung zu einem bestimmten Sachverhalt gegeben werden soll.

Eine informierte Einwilligung sollte in der Sprache der Person erfolgen. Wenn Bildschaffende nicht die Sprache oder den Dialekt der Abzubildenden/Abgebildeten sprechen, sollten Dolmetscher:innen Teil des Projektteams sein. Zu beachten ist auch, dass den Betroffenen datenschutzrechtlich weitere Informationen erteilt werden und die Zugänglichkeit zu Informationen, die Verständlichkeit und die Lesbarkeit von Datenschutzinformationen gewährleistet werden müssen.

Erfolgt die Datenverarbeitung mit Einwilligung der betroffenen Person, sollten die Verantwortlichen diese auch nachweisen können. Es steht ihnen frei, Methoden auszuarbeiten, um diese Bestimmung auf eine Weise einzuhalten, die zu ihren täglichen Geschäftstätigkeiten passt. Zugleich sollte dies nicht zu einer übermäßigen Erhöhung des Datenverarbeitungsvolumens führen. Die Verantwortlichen sollen also nicht mehr Informationen erheben, als erforderlich ist, um den Zweck der Verarbeitung zu erfüllen.

[24] Rosenthal, Das neue Datenschutzgesetz, Jusletter 2020.

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

[26] Hinweis: Dies gilt zwar nach Schweizer Recht nicht ausdrücklich, aber zwingend nach Art 7 DSGVO. Die Einwilligung muss genauso leicht widerrufbar sein, wie sie erteilt worden ist. Weitere Vorgaben zum Prozess des Widerrufs bestehen nicht.

[27] Vgl. dazu Art. 21 Abs. 3 lit b DSG.

Beispiel Fairpicture Consent App

Einwilligungsverfahren bedeuten einen gewissen Mehraufwand. Technische Lösungen, die oben beschriebene verpflichtende Aspekte der Einwilligung einfach umsetzbar machen wie beispielsweise die Fairpicture Consent App, vereinfachen die Prozesse für Organisationen und Bildschaffende. Die Fairpicture Consent App enthält die Angaben zur Einwilligung in mehreren Sprachen sowohl in schriftlicher Form als auch abspielbar als Audiodatei. Die Bildschaffenden werden Schritt für Schritt durch die Verzweigungen im Prozess der Einwilligung geführt. Die Porträtierten haben die Möglichkeit, ihre Einwilligung auf verschiedene Arten zu geben, zum Beispiel per Geste, die in der App dokumentiert wird, oder mit ihrer Unterschrift. Die Einwilligung wird außerdem direkt mit den Bildern abgelegt.

1.4.4 Einwilligung von/für Kinder

Kinder sind hinsichtlich der Verarbeitung von personenbezogenen Daten als besonders schutzwürdig einzuordnen. Das kann etwa im Schulkontext bedeuten, dass zwar die Lehrperson und die Schulleitung das Einverständnis erteilen, dass in der Schule fotografiert/gefilmt werden darf. Sie werden jedoch auch verpflichtet, die Eltern entsprechend zu informieren. Wenn die Eltern nachträglich nicht einverstanden sind, können sie die Löschung der Daten verlangen. Deshalb müssen von jedem fotografierten/gefilmten Kind (Protagonist:in) die Daten erhoben werden.[28]

Bei der Erfassung, Verwaltung und Nutzung von Inhalten, in denen Bildmaterial von Kindern verarbeitet wird, ist mit besonderer Sorgfalt vorzugehen. Folgendes ist zu berücksichtigen: Bewertung des Risikos für das Kind (mit besonderer Sorgfalt für speziell gefährdete Kinder); Sicherheit des Kindes; Achtung der Rechte, der Integrität und der Würde des Kindes; Einholung und Dokumentation der informierten Einwilligung des Kindes (wenn altersbedingt möglich) sowie der Einwilligung seiner Eltern oder des Vormunds.

1.4.5 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 (wenn in einer von der fotografierten/gefilmten Person unterschriebenen Vereinbarung das Erstellen und die Verwendung von Bildern bereits geregelt ist, zum Beispiel in einem Arbeitsvertrag (Vertragserfüllung als Rechtsgrundlage));

- 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 (z.B. unmittelbar nach Notsituationen) wird die Einholung einer Einwilligung nicht möglich sein. Wenn sich aus dem Bild oder aus dem bekannten Kontext keine

[28] Siehe dazu beispielhaft: https://www.forschungsdaten-bildung.de/files/rekrutierung_aufklaerung_fuer_kinder.pdf.

besonders schutzwürdigen Daten ergeben, ist die Einholung der Einwilligung zumindest nach dem Schweizer Recht auch nach dem revidierten DSG in der Regel nicht erforderlich.

1.4.6 Widerruf als zentraler Bestandteil der Einwilligung

Dem Widerruf der Einwilligung wird in der DSGVO eine herausragende Stellung eingeräumt. Demgegenüber gibt es nach dem DSG terminologisch nur ein Widerspruchsrecht, aber kein spezielles Widerrufsrecht gegen Einwilligungen. Im Ergebnis ist der Widerruf im Sinne der DSGVO mit dem Widerspruch im Sinne der DSG aber vergleichbar. Nach der DSGVO müssen Verantwortliche sicherstellen, dass die betroffene Person die Einwilligung jederzeit widerrufen kann und der Widerruf der Einwilligung so einfach sein muss, wie deren Erteilung.[29] In der DSGVO ist nicht festgelegt, dass das Erteilen und Widerrufen der Einwilligung immer durch dieselbe Handlung erfolgen muss. In der DSGVO wird das einfache Widerrufen für eine gültige Einwilligung als notwendig erachtet. Wenn das Widerrufsrecht die Anforderungen der DSGVO nicht erfüllt, steht der Einwilligungsmechanismus der Verantwortlichen nicht im Einklang mit der DSGVO.

Daher: Wenn der Widerrufsprozess nicht gewährleistet werden kann, kann keine rechtlich gültige Einwilligung zustande kommen!

1.5 Die Rechte von in Bildern und Videos abgebildeten Menschen

1.5.1 Recht auf Information

Die Informationspflichten gemäß der DSGVO schreiben vor, dass Betroffene vor oder mit der Datenerhebung informiert werden müssen, was mit ihren Daten passiert.[30] Das bedeutet in der visuellen Industrie oftmals zusätzlichen Aufwand und in gewissen Fällen sind Informationspflichten schwer umzusetzen. Informationen müssen zugänglich, verständlich und lesbar sein.
Daher schlagen die Aufsichtsbehörden der DSGVO ein zweistufiges Informationsmodell vor.

Beispiel Fairpicture Consent App

Damit die Betroffenen ihre Einwilligung zurückziehen können, müssen sie wissen, an wen sie sich in diesem Fall wenden können – und dies muss einfach machbar sein. Um sich äußern zu können, erhalten Abgebildete optimalerweise die Kommunikationsmaßnahmen zu sehen, auf denen sie abgebildet sind. Im Fall des Rückzugs der Einwilligung müssen die Verantwortlichen in der Lage sein, diesen Widerruf auch rechtskonform umzusetzen. Dafür braucht es klare Datenstrukturen – es muss eindeutig sein, wo welche Bilder für wie lange in Verwendung sind. Die Nachverfolgung von Bildern und Videos im Internet ist in vielen Fällen nicht möglich, was diesen Vorgang erschwert.

Fairpicture arbeitet an Lösungen für diese Problematik. Die Fairpicture Consent App bietet einfache Möglichkeiten für den Widerruf von Einwilligungen. Mithilfe neuer Ansätze wie etwa der c2pa soll es möglich werden, bei einer Veröffentlichung online anzuzeigen, ob für ein bestimmtes Bild eine Einwilligung vorliegt, weil diese kryptographisch verschlüsselt direkt im Bild abgespeichert werden kann.

In der ersten Stufe sollen Basisinformationen gegeben werden, die der betroffenen Person den Umfang der Datenverarbeitung bewusst machen. Dazu gehören:

- Name und Kontaktdaten des/der Verantwortlichen;
- Kontaktdaten des/der Datenschutzbeauftragten (soweit benannt);

[29] Art 7 Absatz 3 DSGVO.

[30] Art 7 Absatz 3 DSGVO.

- Verarbeitungszwecke und Rechtsgrundlage in Schlagworten;

- Empfänger:in oder Kategorien von Empfänger:innen der personenbezogenen Daten;

- Übermittlung in Drittstaaten (für uns: grundsätzlich weltweite Nutzung);

- Aufklärung über das Recht auf Widerspruch.

In der zweiten Stufe soll auf ausführliche Datenschutzhinweise verwiesen werden (zum Beispiel auf der Website). Durch dieses zweistufige Informationsmodell lässt sich die Vielzahl der gesetzlich vorgeschriebenen Informationen in einer Art aufteilen, die in den meisten Fällen umsetzbar ist. Die Zugänglichkeit zu Informationen, die Verständlichkeit und die Lesbarkeit von Datenschutzinformationen stellen häufig ein großes Problem dar. Die Transparenzanforderungen der DSGVO können nicht wirksam erfüllt werden, wenn die Botschaft nicht bei den Betroffenen ankommt.[31] Die Verständlichkeit ist dabei eng mit der Forderung nach einer klaren und einfachen Sprache verbunden. In der Praxis heißt das, bei der Verwendung einer schriftlichen Form vor allem darauf zu achten, welche Sprache die Betroffenen verstehen, welche Komplexität im Hinblick auf den Bildungsgrad die verwendete Sprache aufweisen darf und ob die Betroffenen lesen und schreiben können. Herrscht bei den Verantwortlichen Unsicherheit bezüglich des Grads der Verständlichkeit bzw. der Transparenz der Informationen sowie der Aussagekraft der Benutzeroberflächen/Hinweise/Strategien etc., können diesbezügliche Tests durchgeführt werden.

Die Kommunikation sollte an die Gewohnheiten/Lebensumstände der Betroffenen angepasst werden (z.B. keine E-Mails schicken oder lange Dokumente zu lesen gegeben, wenn die Betroffenen Probleme haben könnten, diese Texte zu verstehen. Vielmehr sollten persönliche Treffen und/oder Sprach-/Videobotschaften genutzt werden). Da personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden dürfen, werden diese vorab zu bestimmen sein und müssen nach Art 13 Abs 1 lit c DSGVO auch entsprechend kommuniziert werden. In welchem Detaillierungsgrad der Zweck gegenüber der betroffenen Person offengelegt werden muss, wird nicht näher bestimmt. Es ist jedoch von einer konkreten, deutlichen und präzisen Formulierung auch aufgrund des Transparenzgebots gemäß Art 12 Abs 1 DSGVO auszugehen. Die Artikel-29-Datenschutzgruppe nennt einige Beispiele für unzureichende Informationen über den Zweck der Verarbeitung:

- „Wir können Ihre persönlichen Daten verwenden, um neue Dienste zu entwickeln."

- „Wir können Ihre personenbezogenen Daten zu Forschungszwecken verwenden."

- „Wir können Ihre personenbezogenen Daten dazu verwenden, personalisierte Dienste anzubieten."

Diese Formulierungen seien nach Ansicht der Artikel-29-Datenschutzgruppe zu unklar. Die betroffene Person verstehe nicht, was tatsächlich mit den personenbezogenen Daten gemacht wird.

Empfehlungen für die Praxis

- Wenn Betroffene eine andere Sprache als die/der Bildschaffende sprechen, muss eine Übersetzung/Verdolmetschung der Informationen und der Einwilligung erfolgen.
- Die Informationen müssen für alle Betroffenen verständlich sein. Sie sollen auf die praktischen Maßnahmen beschränkt sein (mit Beispielen aus dem Leben der Betroffenen).
- Es sollte bei einigen wenigen Personen getestet und überprüft werden, ob die Botschaften verstanden worden sind.

[31] Art 15 DSGVO.

In diesem Zusammenhang ist anzunehmen, dass die Angabe über die „Erstellung und Verwendung eines Bildes für die Kommunikation“ einen zu geringen Informationsgehalt hat. Deshalb ist in Bezug auf die Umstände näher einzugehen, wofür die Bilder Verwendung finden. Für eine rechtskonforme Information über die Zwecke ist somit die Kontextinformation, unter der die Bilder erstellt, gespeichert und verwendet werden, anzugeben. Spezifisch genug wäre demgegenüber, den Kontext jeweils konkret pro Projekt zu kommunizieren. In der Kombination ergäbe sich dann z.B.: „Verwendung der Bilder in der Kommunikation im Kontext von Entwicklungszusammenarbeit auf der Website, in Social Media und in gedruckter Form.“

Der Kontext ist deshalb von Bedeutung, weil er den Zweck der Verarbeitung mitbestimmt. Der Transparenzgrundsatz setzt voraus, dass für Betroffene klar ist, für welchen Zweck ihre Daten verarbeitet werden. Welche Bedeutung einem Bild allerdings zugemessen wird, ist erst deutlich, wenn der Kontext bekannt ist, in den das Bild eingebettet wird. Erst mit den wesentlichen Zusammenhängen der geplanten Darstellung lässt sich beurteilen, ob die Verwendung des Bildes mit einer berechtigten Erwartungshaltung der Betroffenen aufgrund der Informationen vereinbar ist.

Um diese Angaben für Bildschaffende zu erleichtern, kann eine ausdrückliche Wiedergabe von Fragestellungen oder Umständen, die z.B. Kategorien wie „Kriegerischer Konflikt“, „Person Öffentlichen Lebens“ o.ä. beinhaltet, bei der Eingabe der Kontextinformation nützlich sein.

1.5.2 Rechte auf Auskunft, Berichtigung und Löschung

Nach der DSGVO sowie dem DSG stehen den Abgebildeten in Bildern und Videos (inklusive der entsprechenden Metadaten) folgende Rechte zu:

- Werden ihre personenbezogenen Daten verarbeitet, so haben sie das Recht, Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten.[32]

- Sollten unrichtige personenbezogene Daten verarbeitet werden, steht ihnen ein Recht auf Berichtigung zu.[33]

- Liegen die gesetzlichen Voraussetzungen vor, so können sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen.[34]

- Wenn sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht ihnen gegebenenfalls ein Recht auf Datenübertragbarkeit zu.[35]

Einwilligungen zur Datenbearbeitung bei Bildern und Videos können jederzeit von den Betroffenen zurückgezogen werden. Der Widerruf wirkt jedoch erst für die Zukunft und nicht rückwirkend. Datenbearbeitungen, die vor dem Widerruf erfolgt sind, sind davon nicht betroffen (dies ist zum Teil auch nicht umsetzbar, zum Beispiel bei gedruckten Bildern). Veröffentlichungen im Internet hingegen können zu jedem Zeitpunkt offline genommen werden, was im Falle eines Widerrufes auch von den Verantwortlichen getan werden muss.

[32] Art 15 DSGVO.

[33] Art 16 DSGVO.

[34] Art 17, Art 18, Art 21 DSGVO.

[35] Art 20 DSGVO.

Bilder können Abgebildete gefährden – wie Risiken minimiert werden können

2 Bilder können Abgebildete gefährden – wie Risiken minimiert werden können

Visuelle Kommunikation birgt potentielle Ri-siken für die Bildschaffenden, die Abgebildeten sowie die kommunizierenden Organisationen selbst. Es ist nicht möglich, alle Risiken auszuschließen, aber eine ernsthafte Risikominderung ist obligatorisch. Um unverhältnismäßige Grundrechtseingriffe zu vermeiden und damit eine rechtskonforme Bildverwendung zu gewährleisten, haben die Verantwortlichen dafür zu sorgen, dass für abgebildete Personen(gruppen) in den entsprechenden Kontexten eine Risikoanalyse vorgenommen wird.[36] Gefährdete Gruppen sollten gesondert beurteilt werden.

2.1 Hintergründe zur Risikoanalyse

Die DSGVO sowie das DSG verfolgen einen risikobasierten Ansatz. Unter Risiko verstehen die Erläuterungen zur DSGVO das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt oder zu einem weiteren Schaden für eine oder mehrere betroffene Person/en führen kann. Verantwortliche 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 (etwa Menschen in Konfliktsituationen, vulnerable Gruppen etc.), sind besondere Maßnahmen wie die Durchführung einer Datenschutz-Folgenabschätzung bzw. eines Human Rights Impact Assessments (Grundrechtsassessments) notwendig.[37]

2.2 Datenschutz-Folgenabschätzung in der Praxis

Risiken für die Abgebildeten sollen grundsätzlich als Produkt von „Eintrittswahrscheinlichkeit“ und „Schwere“ des Nachteils beurteilt werden. Dabei wird zwischen „physischen“, „materiellen“ und „immateriellen“ Schäden unterschieden.[38] In der DSGVO werden exemplarisch u.a. Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung und unbefugte Aufhebung der Pseudonymisierung angeführt. Dabei wird auch auf andere erhebliche wirtschaftliche und gesellschaftliche Nachteile verwiesen, die durch die Datenbearbeitung entstehen können (etwa wenn Abgebildete daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren oder personenbezogene Daten schutzbedürftiger natürlicher Personen verarbeitet werden).[39]

> Das Research Institute unterstützt Organisationen bei der Durchführung von Datenschutz-Folgenabschätzungen.[40]

Die Methodik der Risikobeurteilung stützt sich im Kern auf die Risk Management ISO-Norm 31000:2018.[41] Darüber hinaus wurde Anleihe am Risk Assessment Leitfaden des deutschen Bundesverbands der Informationswirtschaft, Telekommunikationsbranche (Bitkom) sowie dem Handbuch für Datenschutz-Folgenabschätzungen des Frauenhofer-Institutes für System und Innovationsforschung genommen. Der Europäische Data Protection Supervisor (EDPS) sieht grundsätzlich keine spezifische Methode zur Durchführung einer DSFA vor, sondern erachtet jede Vorgehensweise für zulässig, die im Einklang mit den Vorschriften der DSGVO und den Leitlinien der Artikel-29-Datenschutzgruppe steht. Der Prozess der Risikobeurteilung lässt sich generisch in die folgenden methodischen Teilschritte unterteilen:[42]

- Risikoidentifikation

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

[36] Art 35 Abs 7 lit c DSGVO.

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

[38] Vgl ErwGr 75 DSGVO.

[39] Vgl ErwGr 75 DSGVO.

[40] Referenz: https://www.roteskreuz.at/fileadmin/user_upload/PDF/Datenschutz/Datenschutz-Folgenabschaetzung-Bericht_OeRK_StopCoronaApp_04-08-2020_V2.0_final.pdf.

[41] https://www.iso.org/standard/43170.html.

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

- Risikoanalyse und -bewertung

(Bestimmung der Eintrittswahrscheinlichkeit und Schwere des Schadens[43]; Bewertung des Risikoszenarios anhand einer Risikomatrix zumindest 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)

2.3 Beurteilung des Risikos durch Kontextinformation

Die Risikobewertung gilt als Herzstück der DSFA. Dabei ist zu beachten, dass konsequent die Perspektive der Betroffenen eingenommen wird. Die Folgen- und Risikoabschätzung ist als Prozess zu verstehen und laufend an die tatsächlichen Begebenheiten und Entwicklungen anzupassen und zu aktualisieren. 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 vulnerable Gruppen stärker bedroht werden). Wenn sich ein Kontext ändert und für die Abgebildeten infolgedessen Menschenrechtsverletzungen zu befürchten sind, müssen die Verantwortlichen Maßnahmen treffen und beispielsweise Bilder aus (insb. online-) Publikationen entfernen.

Zur Beurteilung des Risikos für die Betroffenen ist die Kontextinformation heranzuziehen. Denn zur Sicherstellung der Zweckbindung sowie der Datenminimierung bzw. -richtigkeit ist einerseits vor der Datenverarbeitung, andererseits regelmäßig eine Überprüfung notwendig. Wenn also Bilder in Verwendung sind, muss es eine kontinuierliche Gefahrenbeurteilung geben für den Fall, dass sich ein Kontext ändert und die damals abgebildeten Personen plötzlich gefährdet sind bzw. ein immaterieller Schaden i.S. einer Menschenrechtsverletzung zu befürchten ist. Bei der Bearbeitung sind vor allem die folgenden Leitfragen zu berücksichtigen.
Die zentralen Fragen für die Risikobeurteilung in der visuellen Kommunikation sind:

- Welche Kontextinformationen sind vorhanden und wie wirken sich diese auf den Einsatzzweck des Bildes aus?

- Wie werden die Gefahren und Risiken für Abgebildete im Moment der Verwendung beurteilt?

Empfehlung zur Kontextaktualisierung

Die Verantwortlichen sollten sich in den Wochen nach dem Produzieren der Bilder und Videos mit den Abgebildeten treffen. Es gilt herauszufinden, was sie von den veröffentlichten Geschichten halten und ob sie Rückmeldungen bekommen haben und Feedback geben möchten (nicht nur bezüglich der Veröffentlichung, sondern auch in Bezug auf den Entstehungsprozess der Bilder und Videos). Das ist für Abgebildete auch eine Gelegenheit, ihre Einwilligung zu widerrufen oder Vorbehalte gegen die Verwendung ihrer Bilder anzubringen. So können die Situation der Abgebildeten überprüft und bei Bedarf zusätzliche Sicherheitsvorkehrungen getroffen werden. Diese Nachbereitung könnte entweder in einem persönlichen Gespräch, bei einem Telefonanruf oder per E-Mail/Chat durchgeführt werden. In sensiblen Kontexten sollten weitere Gespräche dieser Art folgen, um die kontinuierliche Risikobeurteilung zu ermöglichen.

[43] 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.

Die wichtigsten Aspekte der Einhaltung menschenrechtlicher Sorgfaltspflichten

Die Verarbeitung von Bildmaterial kann mitunter zu besonders hohen Risiken für die abgebildeten Personen führen.

Für jede Verarbeitung muss eine Identifikation der mit der Verarbeitung verbundenen Risiken erfolgen (Risikoanalyse).

Bei der Risikoanalyse muss eine nachvollziehbare Einordnung erfolgen, ob es sich um ein hohes Risiko handelt oder nicht.

Für besonders risikoreiche Verarbeitungstätigkeiten sieht die DSGVO (als Ausfluss des risikobasierten Ansatzes) die Verpflichtung zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA) bzw. Human Rights Impact Assessment (HRIA) vor.

Im Hinblick auf die oben aufgeführten Gründe sollte eine Schwellwertanalyse anhand der Kriterien des Art 35 DSGVO und der Leitlinien des Europäischen Datenschutzausschusses (EDSA) erfolgen.

Ist das Ergebnis der Schwellwertanalyse positiv und liegt voraussichtlich ein hohes Risiko vor, sollten eine Datenschutz-Folgenabschätzung bzw. ein Human Rights Impact Assessment erfolgen.

Die Risikoanalyse hat nicht nur vorab, sondern kontinuierlich (zyklisch sowie situationsabhängig) zu erfolgen. Dabei ist die Kontextinformation der Bilder zu berücksichtigen.

Nützliche Links

Artikel-29-Datenschutzgruppe, Stellungnahme 15/2011 zur Definition von Einwilligung (WP187)
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_de.pdf

Art-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, wp248rev.01
https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47711

Art-29-Datenschutzgruppe, Leitlinien für Transparenz (WP260 rev.01)
https://www.dsb.gv.at/dam/jcr:17cb6862-7bc0-4039-8c47-97bc09602214/Leitlinien%20f%C3%BCr%20Transparenz%20gem%C3%A4%C3%9F%20der%20Verordnung%202016-679.pdf

EDSA, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf

EDSA, Leitlinien 05/2020 zur Einwilligung:
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf

EDSB, Rechenschaftspflicht in der Praxis Teil II: Datenschutz-Folgenabschätzung und vorherige Konsultation
https://edps.europa.eu/system/files/2021-07/19-07-17_accountability_on_the_ground_part_ii_en_445_de.pdf

Europäische Menschenrechtskonvention
https://www.echr.coe.int/documents/convention_deu.pdf

ISO 31000:2009 Risk management — Principles and guidelines
https://www.iso.org/standard/43170.html

Oxfam, Ethical Content Guidelines:
https://policy-practice.oxfam.org/resources/ethical-content-guidelines-upholding-the-rights-of-the-people-in-the-pictures-i-620935/

Grundrechte-Charta der Europäischen Union
https://www.europarl.europa.eu/charter/pdf/text_de.pdf

Weiterführende Literatur

Weiterführende Literatur

Dieses Paper wurde auf Basis einer umfassenden, wissenschaftlichen Ausarbeitung erstellt. Zur besseren Lesbarkeit wurde auf eine detaillierte Zitation verzichtet, jedoch möchten wir die Literaturquellen, derer wir uns bedient haben, nicht ungenannt lassen.

Bitkom, Risk Assessment & Datenschutz-Folgenabschätzung (2017)

Bock et al, Datenschutz-Folgenabschätzung für die Corona-App (2020)

Buchner/Petri in Kühling/Buchner, DS-GVO/BDSG2 (2018)

Feiler/Forgó, EU-DSGVO (2022)

Frenzel in Paal/Pauly, DSGVO/BDSG2 (2018)

Gosch, Zur Reichweite der Klassifizierung sensibler Daten, JusIT 2022/76

Kastelitz/Hötzendorfer/Tschohl in Knyrim, Der DatKomm (2022)

Knyrim in Ehmann/Selmayr, DS-GVO2 (2018)
Rosenthal, Das neue Datenschutzgesetz, Jusletter 2020

Schantz in Schantz/Wolff, Das neue Datenschutzrecht (2017)

Schulz in Gola, DS-GVO2 (2018)

Martin et al, Datenschutz-Folgenabschätzung (2020)

Trieb in Knyrim, DatKomm (2019)

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.