Quick Guide

How to visually communicate in a data protection-compliant way

A practical introduction

fairpicture

research institute

Anyone who produces visual material and uses it to communicate should be aware of the General Data Protection Regulation (GDPR) and other data protection regulations[1]. However, the legal framework of communication with visuals is often ignored by many organisations, which leads to consequences for those depicted, for the visual creators and the publishing organisation. Photographs and videos can be personal, sensitive or even biometric data, which leads us to the topic of data protection. The production of and communication with visual material also entails various risks that might not be apparent at first glance. Raising awareness of legally binding risk analyses and the consent of those depicted, which is mandatory in certain cases, are important steps towards visual communication that complies with data protection requirements.

This is a summary of a white paper produced by Research Institute and Fairpicture. The detailed document with more background information can be downloaded here:

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

To assess the legal requirements that must be met when creating and publishing visual material, it is important to distinguish between different categories of data.

Visual material is personal data if the person(s) depicted can be identified. Personal data can be divided into (1) «normal» personal data and (2) special category data/data particularly worthy of protection (hereinafter «sensitive data»). Information that directly reveals the identity of the individual is referred to as «primary identifier». Other information that can be directly assigned to the identified person is also to be considered personal data. In other words, if a person's name is processed (which is often the case with photographs and videos with contextual data), it is personal data. All other information that can be taken from the visual material also becomes personal data.

Sensitive data are personal data if they reveal information such as ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. Sensitive data also includes the processing of genetic or biometric data to uniquely identify a natural person, health data or data concerning a natural person's sex life or sexual orientation.

Stricter requirements apply to the processing of sensitive data. For example, processing is not permitted even on the basis of legitimate interests of the media and the public and explicit consent is generally required. Sensitive data require special security measures and, under certain circumstances, a mandatory data protection impact assessment.

However, photographs and videos are not automatically sensitive data. Visual material showing a person wearing glasses or in a wheelchair is not sensitive per se. In light of the recent case law of the Court of Justice of the European Union (CJEU), this could be assessed differently in the future and the scope of sensitive data in the area of visual material could be opened earlier. If photographs and videos specifically relate to sensitive categories of data (if they reflect, for instance, health data, physical or mental limitations, sexual orientation, ethnic origin, ideological or political beliefs), they become sensitive data in any case.

[1] In Switzerland, the new Act on Federal Data Protection (nFADP) will come into force on 1.9.2023. We recommend using the standards of the GDPR as a benchmark for visual communication in Switzerland as well. According to the Swiss FADP, data processing is permitted, but the seemingly open approach is considerably restricted by further regulations and thus approximated to the DSGVO.

[2] For example, exercising specific fundamental rights such as freedom of expression, freedom of the press and freedom of broadcasting.

Visual material is also not automatically a biometric datum. It only becomes one when special technical processing is used to identify a person, such as in facial recognition.

It follows from the GDPR that any processing of personal data is prohibited unless a legal basis[3] such as consent justifies the data processing. For the processing of non-sensitive personal data, Art 6 GDPR contains an exhaustive list of six legal bases that allow data processing:

- the affected person has given consent to processing for specific purposes;
- processing is necessary for the performance of a contract;
- processing is necessary for compliance with a legal obligation;
- processing is necessary for the protection of vital interests;
- processing is necessary for the performance of a public task;
- processing is necessary for maintaining the legitimate interests of the controller or of a third party.

Elsewhere in the GDPR[4], there are those legal bases which are required for the lawful processing of special categories of personal (or sensitive) data. Since the legislator assigns a higher degree of protection to these data, increased requirements exist for the legal basis for the processing of special categories of personal data.

In this case, the special justifications according to Art. 9 GDPR must be applied. According to the Swiss FADP, data processing is permitted and therefore does not require permission or consent. The law, however, has strict requirements for the processing of personal data. In particular, the data processing must not unlawfully harm the personality of the affected person (Art. 30 FADP). A violation of personality is unlawful if it is not justified by the consent of the affected person, by an overriding private or public interest or by law (Art. 31 FADP). This considerably restricts the seemingly open approach of further regulations and brings it closer to the GDPR, which requires a legal basis for every processing of personal data (Art. 6 GDPR).

[3] See Art. 6, 9 or 10 GDPR.

[4] Art. 9 para 2 GDPR; cf. Art. 3 lit c GDPR – «personal data requiring special protection».

When is it allowed to process sensitive data in visual communication?

Photographs and videos may only be published if they meet one of the following conditions:

- there is an explicit consent of the affected person (declaration of consent);
- internal processing by non-profit organisations takes place;
- visual material is processed that has obviously been made public by the affected people themselves, without them having expressly prohibited processing;
- processing is necessary for the establishment, exercise or defence of legal claims or in case of action by the courts;
- there exists a substantial public interest
- processing is necessary for archiving, research or statistical purposes in the public interest.

Handling personal and sensitive data requires a great deal of care and operates within a binding legal framework.

The importance of this becomes even clearer when the risks are considered that visual communication with personal and sensitive data poses for the visual creators, for those depicted and for the communicating organisations themselves. It is not possible to eliminate all risks, but risk mitigation is legally obligatory. What does this mean in practice?

Legally binding risk analysis in visual communication

Any production and processing of personal data such as photographs involves risks. Therefore, risk assessment is crucial. Everyone who produces or processes personal visual material must consider the possible risks to the rights and freedoms of the persons depicted. The GDPR and the FADP take a risk-based approach to this. Controllers[5] are obliged to conduct a risk analysis. The technical and organisational measures must consider the risks to the rights and freedoms of persons depicted. If there are high risks for the persons depicted (e.g. people in conflict situations or members of vulnerable groups), special measures such as conducting a data protection impact assessment or a human rights impact assessment are necessary[6]. The aim is to avoid risks for the fundamental and human rights of the persons depicted and the visual creators or to reduce them to an acceptable minimum.

Possible physical, material or immaterial harm is:

- threat of violence
- discrimination
- identity theft or fraud
- financial loss
- damage to reputation
- unauthorised removal of pseudonymisation
- other significant economic or social harm.

The risk assessment process can be divided into the following methodical sub-steps[7]:

- risk identification (description of the scenario, identification of persons involved and affected, identification of the risk source)

- risk analysis and assessment (determination of the probability of occurrence and the severity of the harm[8]; evaluation of the risk scenario on the basis of a risk matrix in high, normal or low)

- risk treatment (consideration of existing technical and organisational risk mitigation measures; determination of additional remedies to further minimise identified risks and reassessment of risk).

In visual communication, it is important to note that the risk context of persons depicted can change significantly (for example, the political situation in a country can change in such a way that certain groups are more threatened). If a context changes and persons depicted have to fear human rights violations as a result, controllers must take measures and, for instance, remove visuals that have already been published where possible.

[5] «Controllers» are natural or legal persons, public authorities, bodies or other entities which alone or jointly with others determine the purposes and means of the processing of personal data. If two or more controllers jointly determine the purposes and means of processing, they are joint controllers and must specify in an agreement in a transparent manner which of them must comply with which obligation under the GDPR (Art. 4 Z 7 GDPR).

[6] See also the FADP under Art. 22, which also provides for mandatory data protection impact assessments under certain circumstances.

[7] See in particular Art. 35(7) and recitals 76, 77 and 83 of the GDPR.

[8] On the process of assessment, recital 76 also states that the likelihood and severity of the risk should be determined in relation to the nature, scope, circumstances and purposes of the processing.

Consent and revocation of consent as a foundation of data protection

Data protection in visual communication is a catalyst for human rights. Often persons depicted know relatively well about their own danger situation, which is a good reason to ask them about it. Moreover, visual stories cover very personal, sometimes sensitive issues. The leading question «If you were the person in this photograph, would you want it to be published?» brings us closer to this topic. Consent has a binding legal basis as an important pillar of the GDPR.

In visual processing, consent is one of the most important legal bases. It is an expression of the self-determination of the affected person under data protection law, who thus decides on the «whether» and «how» of data processing. All people have the right to their own image and the right to privacy. By giving consent to the production and processing of their visuals, they become active participants in communication and have agency over their visual representation.

While the FADP does not contain any explicit regulations on the design of consent, the GDPR makes very detailed specifications[9]. These concern principles that are largely transferable to the Swiss legal situation.

Principles of consent and its revocation

For consent to be legally valid, it must be voluntary[10]. It always applies only to the specific case and purpose and is given in full knowledge of all circumstances. Consent is an unequivocal expression of will in the form of a declaration or other unambiguous affirmative action. The affected person thereby indicates that he or she consents to the processing of personal data relating to him or her. This expression of will can be a signature, but also an unambiguous gesture or verbal consent recorded by video, for example.

In the GDPR, the right to simple revocation is considered necessary for valid consent. If this right does not meet the requirements of the GDPR, the consent mechanism of controllers is not in line with the GDPR. People who give consent must also be able to revoke it. They need to know how to easily contact the controllers and have the right to have their data deleted and, where possible, withdrawn upon revocation.

If the revocation process cannot be guaranteed, no legally valid consent will be given!

[9] See also: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf

[10] As the Art. 29 Working Party has stressed in various opinions, consent can only be valid if the affected person has a genuine choice and there is no risk of deception, intimidation, coercion or significant adverse consequences should he or she not give consent.

When is consent not required?

There are situations in which consent is not necessary, is particularly inconvenient or even impossible. According to the GDPR and the FADP, the following exceptions define situations in which consent of the person depicted is not necessary:

- the recording and publication are part of a contract signed by the affected person;
- the persons depicted are not identifiable already at the time of recording (anonymous data, data protection law is not applicable);
- controllers can rely on a legal basis that allows or requires the processing of the visual material;
- controllers have a legitimate interest that makes the processing necessary and the fundamental rights of the affected person do not conflict with this (note: this exception does not apply to sensitive data and in relation to children!).

In some situations, obtaining consent will not be possible. If the visual material or the known context does not reveal any data that is particularly worthy of protection, obtaining consent is usually not necessary, at least under Swiss law.

Read more in the detailed version

This document introduces the data protection implications of visual communication. The white paper goes into more detail on the topics touched upon. It can be downloaded under the following link:

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

About the authors

fairpicture

Fairpicture offers fair photo and video assignments that meet ethical and legal criteria for visual communication. They develop the infrastructure, for example the Fairpicture Consent App, to carry out consent processes in a legally compliant and easy manner for all parties involved. Furthermore, Fairpicture advises companies on topics such as fair and ethical visual communication.

research institute

Research Institute AG & Co KG advises organisations on data protection issues relating to visual communication. Much experience in preparing data protection impact assessments and human rights impact assessments flows into their consultations.