University of Zurich[UZH]

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

Center for Information Technology, Society, and Law (ITSL)

ScanVan
Data Protection Analysis

Report of 2 November 2020

Prof. Dr. Florent Thouvenin
Dr. Aurelia Tamò-Larrieux
Kento Reutimann

Zurich, 2 November 2020
Version 2.1 – updated for publication on 26 April 2021

Table of Contents

I. Introduction

When Google introduced Street View in 2009, any internet user gained access to information that was entirely unimaginable before. Street View makes it possible to explore well-known as well as remote places all over the world through a web-based platform. This vast amount of freely available 360° images enable any user to find directions or to explore new places. However, the lack of depth information makes Street View unsuitable for many applications. A systematic 3D digitalization of (urban) environments is therefore of great interest for both governments (e.g., for city planning purposes) and private entities (e.g., to enable drone deliveries). In Switzerland, cutting-edge research in this field is being conducted at the EPFL within the ScanVan project, which is funded by the Swiss National Science Foundation within its National Research Program 75 on Big Data (NRP75).

Within the scope of the NRP75 ScanVan project, we were mandated by the EPFL in the spring of 2020 to assess the technology and its potential implementations from a data protection perspective. In this memorandum, we discuss the data protection requirements that apply with respect to the processing of data that is necessary to create 3D point clouds. Aside from elaborating on individual data protection law requirements, concrete design recommendations will be made. Primarily, our focus rests on the ScanVan project and the 3D model of the city of Sion. Nevertheless, as the scope of potential future use cases is broad, the main part of our analysis (III. General Legal Analysis) also includes considerations with regard to the design and application of the technology in other use cases. This analysis is therefore of relevance not only to this specific project and technology but to 3D modeling technology in general. In Switzerland alone, multiple research projects on creating digital duplicates of cities exist[1].

The legal analysis will be mainly based on Swiss and European law. In Switzerland, the revised Data Protection Act has passed the legislative process and will come into force soon[2]. We rely on the revised Data Protection Act as adopted by the Swiss Parliament (revDPA) and leave aside cantonal data protection laws. Furthermore, we will make reference to the Swiss Federal Supreme Court's landmark decision with regard to Google Street View[3], rendered in 2012. While this decision set certain boundaries to how the service may be operated, the court ultimately came to the conclusion that the service is in principle legal and in line with the Swiss data protection laws. This decision provides important guidance for the legal analysis of the ScanVan project because the collection of image data using a camera setup mounted to the roof of a moving car is similar in both cases. Reference to this decision will therefore be made in various sections throughout this memorandum.

In the European Union (EU), the General Data Protection Regulation (GDPR) serves as uniform data protection law among its member states. However, the GDPR allows member states to deviate from and substantiate certain specific provisions and sometimes refers to national member state laws. In these cases, the national provisions of member states will have to be considered with regard to the future application of the technology in the EU.

Lastly, it is assumed for both the analysis under Swiss and EU law that personal data is not transferred to any country outside Switzerland or the EU.

1 Cf. e.g. the research project of the University of Applied Sciences and Arts Northwestern Switzerland, SmartMobileMapping, <www.fhnw.ch/de/die-fhnw/hochschulen/architektur-bau-geomatik/institute/institut-geomatik/forschung/smartmobilemapping>; cf. outside of academia iNovitas, <https://www.inovitas.ch>; cf. outside of Switzerland in particular Leica Pegasus, <https://leica-geosystems.com/de-ch/products/mobile-sensor-platforms/capture-platforms/leica-pegasus_two>.

2 The Swiss Parliament adopted the final text on 25 September 2020. The effective date will be determined by the Federal Council after expiry of the 100-day referendum period.

3 BGE 138 II 346.

II. Technical Background

The ScanVan project aims at generating 3D point clouds of cities from images taken by a unique spherical camera. The imaging setup consists of two cameras pointing towards a spherical mirror placed in the middle. This generates two images with a resolution of 3000 x 2000 px each, resulting in a stitched 360° image with a total resolution of 6000 x 2000 px. We are not aware of any plans to increase the resolution of these cameras in the future.

The imaging setup is attached to the roof of a car that drives around the target area. The camera is mounted around 30 cm from the roof on top of the car. A standard estate car is used for the scanning process (roof height approx. 1.5 m), meaning that the camera is mounted at a total height of around 1.8 m above ground. Images are taken every 5 m. Using photogrammetry, the images are used to generate a 3D point cloud of the captured area: The system detects key points within the individual images and compares these points with those found within images taken nearby. Based on the differences between the corresponding key points, the system may then estimate the distance between key points and ultimately their location within the 3D point cloud. This calculation process is fully conducted on a computer located within the vehicle.

Once the vehicle returns, both the original raw images as well as the generated 3D point clouds are downloaded from the vehicle to a server, where the newly generated 3D point cloud is then combined with existing 3D point clouds to generate a complete model.

EPFL also started the development of an anonymization method based on machine learning on the image level. This process shall be applied to the original image data and the calculation of the final 3D point clouds shall then be based on the anonymized image data. The accuracy of the anonymization process is highly dependent on the training of the algorithm. At the end of 2020, the algorithm is planned to provide a relatively high accuracy (> 90 %) for common situations but may be less accurate with regard to unusual street scenes (< 60 %).

III. General Legal Analysis

A. Material Scope

1. Personal Data, Sensitive Personal Data, Anonymized Data

The notion of "personal data" is crucial because data protection laws are (only) applicable if personal data is processed. Personal data is any data that relates to an identified or an identifiable natural person, called *data subject*. This is the case if it is possible to distinguish an individual from others. Identifiers may for example be the name, the birth date, an identification number, or an IP address. When assessing whether an identification is possible, the possibility to combine data with other data must be taken into account. According to the relative approach to personal data, a natural person is identifiable if an identification is possible by means reasonably likely to be used by the data controller or processor (for terminologies, cf. Section III.B). For instance, the European Court of Justice has decided that dynamic IP addresses must be considered personal data if the data controller has the legal means to obtain additional information from internet access providers which allows him to identify the data subject[4]. The means reasonably likely to be used vary depending on the specific case.

Within personal data, "sensitive personal data" constitutes a special category. The processing of this sensitive personal data requires the compliance with additional requirements, such as higher standards with regard to consent by the data subject. According to the revDPA and the GDPR, the following data is considered to be sensitive:

revDPA (CH)	**GDPR (EU)**
data concerning **racial or ethnic origin**	data revealing **racial or ethnic origin**
data concerning **political views or activities**	data revealing **political opinions**
data concerning **religious or philosophical views or activities**	data revealing **religious or philosophical beliefs**
data concerning **trade union views or activities**	personal data revealing **trade union membership**
genetic data	**genetic data**
biometric data that unambiguously identify a person	**biometric data** (where used for identification purposes)
data concerning **health**	data concerning **health**
data concerning the **intimate space**	data concerning **sex life**
	data concerning **sexual orientation**
data concerning **administrative and criminal prosecutions or sanctions**	
data on **social assistance measures**	

Personal data can be pseudonymized or anonymized. A pseudonymization process leads to a state where "personal data can no longer be attributed to a specific data subject without the use of additional information" (Article 4 Paragraph 5 of the GDPR)[5]. The additional information must be kept separately from the identifiable data. According to Recital 26 of the GDPR, as the pseudonymized data could be attributed to a natural person by the use of additional information, such data is still considered to be personal data. Pseudonymization does not exempt the data from the scope of data protection law but it may be an instrument to ensure compliance with the data protection principles, such as the principle of data minimization. As the ScanVan project does not aim at analyzing any data about individuals depicted in the original images (not even statistically), we will not go into more detail about pseudonymization.

4 CJEU judgement of 19 October 2016, C-582/14, Breyer vs. Bundesrepublik Deutschland, Paragraph 49.
5 Pseudonymization is not explicitly mentioned in the Swiss revDPA. However, pseudonymization is still recognized by data protection authorities and may play a role with regard to the adequacy of data security measures (cf. Section III.D.5).

Unlike with pseudonymization, anonymization results in data where an attribution to a natural person is not possible anymore. In case personal data is anonymized, it is not considered to be personal data and falls out of the scope of data protection laws (however, cf. Article 11 of the GDPR). A full anonymization therefore has the benefit that the requirements of the data protection laws do not have to be met anymore, which facilitates the use of such data. In case data may not be fully anonymized, the data protection laws remain applicable; however, partial anonymization may still be relevant in the context of the principle of data minimization (cf. Section III.D.3) or to demonstrate overriding interests (cf. Section III.E).

2. Personal Data within the ScanVan Project

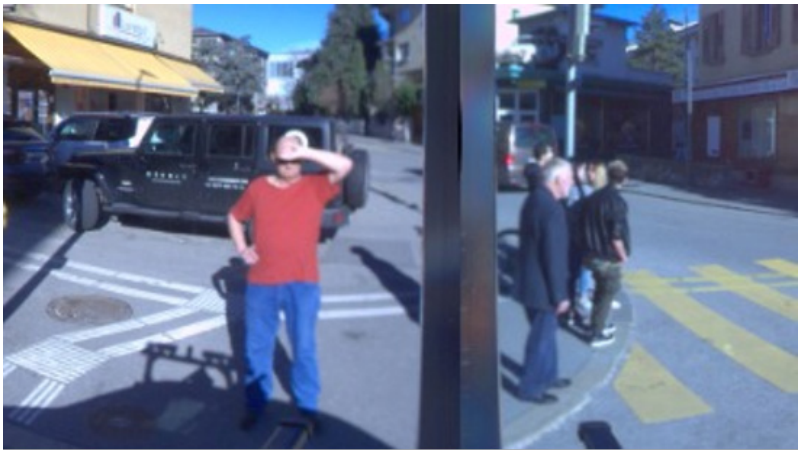
In the ScanVan case, two categories of data may constitute personal data and need to be assessed in more detail:

– Original image data: image data that is captured by the spherical camera.

– 3D point clouds: data resulting from the original image data by means of photogrammetry.

a) Image Data

The spherical camera captures 360° images of the surroundings of the car it is mounted on. People and license plates may be clearly visible. The images contain a considerable amount of details. It is possible to clearly recognize faces of people, their clothing, and their skin color. Furthermore, from the environment, it may also be possible to see what they were doing at a specific time or to draw conclusions about their health (e.g., if someone uses crutches or is exiting a hospital) or attitude towards religion (e.g., if someone is at the entrance of a church). It is therefore highly likely that certain individuals depicted in the image data may be identified and the image data must therefore be considered to be personal data.



As the images contain many details, it must also be analyzed whether the image data may for example be considered to be data concerning racial or ethnic origin, religious beliefs, or health, and therefore sensitive personal data. According to Recital 51 of the GDPR, photographs are not considered sensitive personal data "as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person". The majority of opinions in the literature in the EU as well as in Switzerland seems to back the view that image data alone does not lead to sensitive personal data, even if the racial

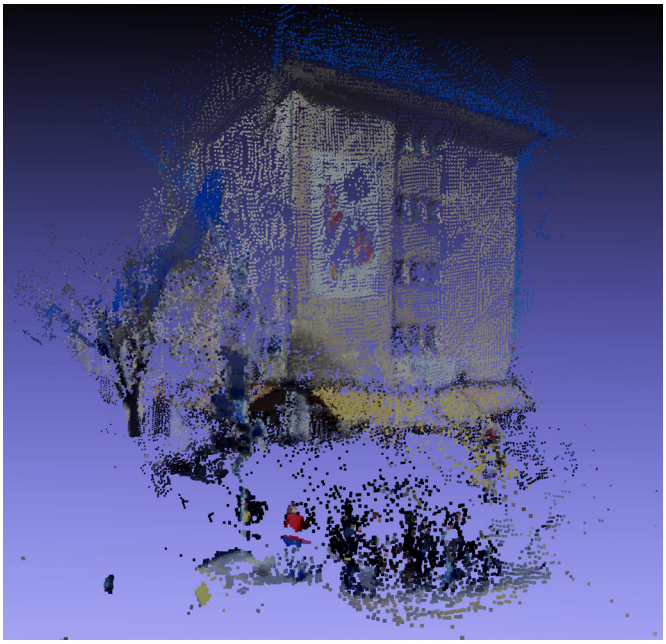
or ethnic background of depicted people may be visible in the pictures, especially if the data – as is the case in the ScanVan project – is not used to draw any conclusions with regard to the depicted individuals[6].

In case an anonymization method is applied, such method would have to be 100 % accurate to fully avoid any personal data. The mechanisms that are currently in development are expected to be very accurate, but it will not be possible to guarantee a full anonymization. While the anonymization process is crucial in light of the data minimization principle (cf. Section III.D.3) and to demonstrate overriding interests (cf. Section III.E), the partially anonymized image data must nevertheless be considered personal data.

In summary, the image data captured by the ScanVan must be considered "normal" personal data.

b) 3D Point Clouds

Based on the image data, 3D point clouds are generated by photogrammetric processes. These calculations are made by computers located in the cars. By comparing different images of a certain area of the city, the algorithms recognize reference points of objects and determine their location in a three-dimensional space, i.e. the 3D point cloud. Color data of these reference points is retained. These calculations rely on the fact that the reference points did not move while the different images were taken; otherwise, the location may not be identified. Reference points that moved are recognized as being inconsistent and are omitted from the 3D point cloud. This means that people and moving cars are usually not included in the 3D point clouds.



Furthermore, the density of the reference points is low enough that faces and license plates will not be recognizable in the 3D point clouds. Therefore, it can be assumed that the 3D point clouds will not contain any personal data.

6 Switzerland: HK-Rosenthal/Jöhri, DSG 3 N 51; cf. also BGE 138 II 346, where the question of whether the image data may be considered to be sensitive personal data was not even mentioned; with regard to the cantonal data protection act of Zurich, cf. Rudin Beat, in: Baeriswyl Bruno/Rudin Beat (eds.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), 2012, IDG 3 N 26; with regard to the cantonal data protection act of Basel-Stadt, cf. Rudin Beat, in: Rudin Beat/Baeriswyl Bruno (eds.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), 2014, IDG 3 N 41. EU: European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on 29 January 2020, Paragraphs 62–65; Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services, adopted on 22 March 2012, Section 4.2; Thilo Weichert, in: Kühling/Buchner (eds.), DS-GVO BDSG Kommentar, 2nd edition, 2018, DSGVO 9 N 3; Gerald Spindler/Lukas Dalby, in: Spindler/Schuster (eds.), Recht der elektronischen Medien, 4th edition, 2019, DSGVO 9 N 4.

B. Terminology: Data Controller and Data Processor

Depending on the role a person (individual or organization) takes in the processing of personal data, such person is considered a *data controller* or a *data processor*. The law prescribes different obligations to data controllers and processors respectively.

A **data controller** is the person who determines the *purposes* for which the data is processed and the *means* of the processing (cf. Article 5 lit. j of the revDPA, Article 4 Paragraph 7 of the GDPR). This control may also be jointly exercised by multiple controllers (= joint controllers).

The **data processor** processes personal data only on behalf of the controller and within the boundaries of the controller's instructions (e.g., a cloud storage provider; cf. Article 5 lit. k and Article 9 of the revDPA, Article 4 Paragraph 8 of the GDPR). As soon as the data processor processes personal data on their own behalf, they also become a data controller. The duties of the processor towards the controller must be specified in a contract or another legal act.

10 The allocation of these roles will have to be made on a case by case basis (cf. Section IV).

C. Territorial Scope

While the revDPA is not limited to data processing within Switzerland, there is no clear-cut rule to determine the applicability of the revDPA[7]. It may be assumed to be applicable in case personal data is processed in Switzerland or the processing of personal data has a connection to Switzerland, for example if the data controller is domiciled in Switzerland or if data subjects have their habitual residence in Switzerland.

The GDPR is also not limited to data processing within the EU borders. It is applicable to processing of personal data in the context of activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU. In addition, it is also applicable to controllers and processors outside of the EU if the data processing is related to the offering of goods or services to data subjects in the EU (irrespective of whether a payment of the data subject is required) or to the monitoring of the behavior of data subjects in the EU. The GDPR in principle does not differentiate between processing by private entities and public bodies.

D. Data Protection Principles

The data protection principles are general rules that trigger different design recommendations depending on a given context (cf. Article 6 of the revDPA; Article 5 of the GDPR). While the GDPR requires the data processing to follow all principles, the revDPA allows non-compliance with these principles to a certain degree if it may be justified (cf. Section III.E). In general, however, the data protection principles are understood very similarly in the revDPA and the GDPR.

1. Lawfulness and Fairness

a) Legal Requirements

According to the **principle of lawfulness**, the data processing shall not be in breach of any laws. The GDPR further requires a valid ground for the processing as specified in Article 6 of the GDPR (cf. Section III.E.2). Similarly, in Switzerland, processing of personal data by a public body requires a legal basis (cf. Section III.E.1).

In practice, it will be very rare that any laws other than data protection laws are violated without being in breach of the data protection laws themselves. As an example, if someone collects data by hacking into a third party server,

7 Article 139 Paragraph 3 of the Federal Law on Private International Law gives claimants a right to choose the applicable law in cases with an international context.

this will most likely be in breach of data protection principles like the principles of transparency and proportionality and, in cases where a legal basis is required, will lack a valid ground (cf. Section III.E). On its own, the principle of lawfulness therefore has limited significance.

According to the **principle of fairness**, personal data shall be processed in a fair manner. The principle of fairness is quite ambiguous and not clearly defined. "Fairness" and "in good faith" are legal terms that are very open to interpretation and are understood differently depending on the circumstances and across different jurisdictions. In general, this principle should be understood as a catch-all provision which may cover situations in which the data subject experiences a disadvantage as a result of the processing of his or her personal data which contradicts the overall balance of power between the data subject and the data controller, without necessarily violating a specific legal prohibition[8].

The Google Street View case was initially brought to the courts by the Federal Data Protection and Information Commissioner, who may start an investigation in cases where the processing of personal data is deemed to be infringing the data protection laws. Having said that, failures to comply with laws other than the Data Protection Act (such as a violation of the general right of personality) do not fall within his competence. As a workaround, in order to still bring up the violation of the general right of personality, the Federal Data Protection and Information Commissioner had to address this topic as part of the principle of lawfulness.

It has to be noted that in Switzerland, data protection is conceptually based on the general right of personality as set out in Article 28 of the Swiss Civil Code (CC). This general right of personality, i.a., also contains the right to one's own image, which in principle establishes that a picture may only be taken or published with the consent of the depicted persons. Having said that, violations of the right of personality, whether caused by an infringement of data protection law or the right to one's own image, may basically be justified for the same grounds of justification (cf. Section III.E.1).

The court found that the right to one's own image was violated but refrained from analyzing possible grounds of justification right away. It rather decided to analyze the justification grounds at once when analyzing the legality of the data processing as a whole because the rights are both based on the right of personality. Ultimately, from the court's decision, it is not clear whether the infringement of the right to one's own image was found to be justified and whether it also constituted a violation of the lawfulness principle.

In practice, as of now, this differentiation should not be too important for the ScanVan project because compliance should be ensured in any case and the grounds of justification are the same with regard to the revDPA and the general right of personality (cf. Section III.E.1). In case the general right of personality is infringed, concerned individuals may base their claims directly on their general right of personality according to Article 28 of the CC, even if such an infringement would not be in violation of the principle of lawfulness.

b) Recommended Actions and Design Considerations

In cases where the technology developed and used in the ScanVan project shall be used in specific economic sectors, it might make sense to have a quick discussion with a lawyer to check compliance with sector-specific laws in order to make sure that the principle of lawfulness is followed. However, if the technology will be used by private companies, it may be expected that these companies are already aware of the relevant requirements and an additional compliance check by a third party may therefore not be necessary.

8 HK-Rosenthal/Jöhri, DSG 5 N 14; Tobias Herbst, in: Kühling/Buchner (eds.), DS-GVO BDSG Kommentar, 2nd edition, 2018, DSGVO 5 N 17.

2. Purpose Limitation and Transparency

a) Legal Requirements

According to the **principle of purpose limitation**, personal data may only be processed for the purpose defined beforehand and communicated to the data subjects. This means that the purpose of the data processing must be defined first and it is not allowed to collect personal data for yet to define purposes. Personal data already collected may only be processed for a different purpose in case certain requirements are met (revDPA: justification, cf. Section III.E.1; GDPR: if the new purpose is compatible with the original purpose, with the consent of data subjects, or if there is a clear obligation or function set out in the law).

The **principle of transparency** prescribes that the data processing is clear to the data subject and that they are informed openly and clearly about the *means and purposes* of the processing. The principle of transparency entails specific information requirements that are specifically set out within the revDPA and GDPR respectively. While under the GDPR the information requirements are broader and more detailed[9], the revDPA mandates that at least following information be provided to the individuals from whom personal data is collected: information on the identity and contact details of the data controller, the purpose of the processing of personal data, and, in case personal data is transmitted or made public to other recipients, information on who receives what categories of data (Article 19 Paragraph 2 of the revDPA).

In the Google Street View decision, the Swiss Federal Supreme Court found that, in order to fulfill the principle of transparency, it is not sufficient that the cameras on top of the car are visible to pedestrians and other individuals[10], even though Google Street View was already well-known at that time. The court stated that even if the cameras are noticed it is not clear to the concerned individuals that the images will be available online for an indefinite period of time.

Furthermore, while Google published information about capturing activities and areas regarding Street View one week in advance, the court found that such information would not sufficiently guarantee the required transparency[11]. Ultimately, the court required Google to publish information about upcoming capturing activities in local media outlets, in particular local newspapers.

b) Recommended Actions and Design Considerations

To fulfill the principle of transparency, the scanning activities should be visible and publicly communicated. The car on which the cameras are mounted could be designed in a way that people may recognize that images are taken, for example by marking the car with camera signs. Information should also be spread via a website, local newspapers, local government agencies, or flyers posted in the city. It is advisable to choose an adequate combination of different information channels to ensure transparency.

The website should provide detailed information on the processing of data (such as, e.g., the anonymization process) so that concerned individuals (or the media) have access to the relevant information. Moreover, a privacy policy should be implemented (usually on the website) that provides information about the processing of personal data. Such a privacy policy should be drafted by a data protection expert in order to comply with applicable laws (especially if the GDPR is applicable).

Furthermore, the exact route of the car may be published on a website so that interested individuals can retrace when the car scans certain neighborhoods. Individuals could then adapt their behavior in order to avoid being photographed. However, if this tracing tool allows to retrospectively determine the time at which a certain image

9 E.g., information on the purposes of processing and legal basis of processing (cf. also below Section III.E), information on the period for which the personal data will be stored, information on how individual can make use of their data subject rights (cf. below Section III.G).
10 BGE 138 II 346, Consid. 9.1.
11 BGE 138 II 346, Consid. 9.1.

was taken, it could reveal the exact point in time at which a depicted individual was at a specific location. This additional information could therefore potentially lead to new data protection problems. As a balancing of interests, Google Street View seems to provide information with regard to the month and year a particular image was taken, but excludes the exact date and time of day. Such an approach could also make sense in the context of the ScanVan project.

3. Proportionality, Storage Limitation, and Data Minimization

a) Legal Requirements

The principle of proportionality is a fundamental requirement for public bodies. It requires that actions by public bodies are appropriate and necessary to achieve an objective in the public interest, and that the objective pursued is proportionate to the burden imposed on private parties (i.e. proportionality in the narrow sense). In the data protection laws, this general principle has been adopted for both private entities and public bodies. Both the purpose and the means of processing must be proportionate.

In the context of data protection laws, the **principle of proportionality** requires that personal data may only be processed to the extent it is objectively suitable and necessary to achieve a specific purpose[12]. Furthermore, the burden imposed by the data processing must be reasonable for the data subject both in terms of its purposes and its means.

The principles of storage limitation and data minimization may be seen as a specific aspect of the principle of proportionality: The **storage limitation principle** requires data to be erased as soon as it is not required anymore to achieve the specified purposes while the **data minimization principle** requires the data processing, including the collection of personal data, to be limited to what is necessary to achieve the specified purposes.

In the Google Street View decision, the court stated that the question of proportionality is very similar to the issue of whether the failure to meet other data protection principles (such as the principle of transparency) may be justified. It therefore analyzed the proportionality as part of the justification grounds (cf. Section III.E.1). The court did not explicitly address the principles of storage limitation and data minimization.

b) Recommended Actions and Design Considerations

The central aim of the ScanVan project is the generation of 3D point clouds; the original image data is only an interim step to achieve this aim. It should therefore be ensured that the original image data is deleted as soon as possible after calculation of the 3D point clouds. Exceptions apply if the original image data still serves a purpose which justifies its retention, such as if the data is kept at EPFL for further improving their photogrammetry methods (cf. Section IV).

If personal image data is retained, further design considerations must be taken into account in order to ensure the proportionality: Sensitive areas (such as hospitals, schools, women shelters) should be identified and excluded from the image capturing process. If such areas are captured, the data gathered in these areas should be fully anonymized as soon as possible (automatically or manually, if required) by blurring individuals and license plates. In other areas, according to the Google Street View decision, an anonymization of at least 99 % may be considered to be sufficient to fulfill the proportionality principle; this anonymization obligation namely applies to faces and license plates[13].

Moreover, compliance with the transparency requirements and enabling data subject rights are key. Data subjects must have the possibility to require removal or anonymization of their data within a reasonable timeframe. The

12 HK-Rosenthal/Jöhri, DSG 4 N 20.
13 BGE 138 II 346, Consid. 10.7.

tools to request removal or anonymization must be designed in an easy-to-use way, for instance through a web form (cf. below Section III.G.2, with illustrations of the approach taken in Google Street View).

4. Data Accuracy

a) Legal Requirements

The data accuracy principle requires the processed personal data to be accurate. This principle is closely linked to the right of rectification (cf. Section III.G).

With regard to the ScanVan project, this principle has little practical importance, as the spherical cameras capture the surroundings objectively, even though the use of mirrors obviously results in a strong distortion. Inaccurate data may emerge in 3D point clouds in the unlikely case that a person is identifiable by combining the 3D point cloud data with other data (e.g. the original image data), and their appearance is represented differently from reality (e.g., an individual appearing much bigger).

14 b) Recommended Actions and Design Considerations

The principle of accuracy will likely not be of major importance. Instead of offering to rectify the inaccurate data, it will be more desirable and easier to remove inaccurate data altogether in case an individual should file such a claim. The requirements with regard to the right to rectification will nevertheless have to be fulfilled (cf. Section III.G).

5. Data Security

a) Legal Requirements

The GDPR requires that personal data is "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')" (Article 5 Paragraph 1 lit. f). The revDPA contains a similar provision that demands the implementation of technical and organizational measures that ensure data security (Article 8 of the revDPA). These measures must be tailored to the security risks associated with the data processing. In Switzerland, the Ordinance to the Federal Act on Data Protection[14] sets out the following goals with regard to data security: physical access to the servers as well as access to the data must be restricted, transmission and transport of data must be secure, access to data must be limited to individuals that require access, and changes to personal data must be protocolled in a manner that allows a retrospective traceability.

b) Recommended Actions and Design Considerations

To ensure compliance with the principle of data security, the data should be stored on an adequately secured infrastructure and access to the personal data should only be granted to individuals that need it for the defined purposes (cf. Section III.D.2). It is key that the measures implemented are well documented in order to be able to demonstrate compliance with the principle of data security. The requirements will have to be assessed on a case by case basis, depending on the sensitivity and volume of the personal data. As the original image data contains more and more detailed personal data than the 3D point clouds, the minimal standards with regard to data security will be higher.

E. Justification and Legal Basis

As mentioned earlier, there is an important difference between the revDPA and the GDPR with regard to the compliance with the data protection principles.

14 Note that the new Ordinance to the revDPA has not yet been published but that it is reasonable to expect similar requirements as currently stated in Article 9 of the Ordinance to the DPA.

On the one hand, according to the revDPA, if the principles are followed, the data processing is considered to be lawful. If not, a failure to do so may still be justified in case the processing is conducted by a private entity (cf. Article 31 of the revDPA). However, in principle, a justification is not possible if public bodies fail to comply with the data protection principles. Even if public bodies fully comply with the data protection principles, there must be a legal basis to process personal data.

On the other hand, according to the GDPR, the principles must be followed in any case. In addition, the GDPR prescribes the need for a valid ground that makes the data processing lawful (cf. Article 6 of the GDPR) that are somewhat similar to the reasons for justification contained in the revDPA.

1. Switzerland

a) Processing by Private Entities

As already mentioned, the revDPA is based on the general right of personality according to Article 28 CC. If the data protection principles are not followed, the revDPA assumes that this general right of personality is violated. No violation is assumed in case the data has been made publicly available by the concerned individual themselves (Article 30 Paragraph 3 of the revDPA). This raises the question whether an individual makes information about their appearance, behavior, and location public by moving in public. Today, cameras are ubiquitous, and people take photos (or selfies) everywhere. It may therefore be argued that individuals in public areas are aware and even expect that they may be photographed and that their photo is published online by people unknown to them, especially on social media platforms. According to the doctrine, Article 30 Paragraph 3 of the revDPA applies only to personal data that was *knowingly* and *willingly* made publicly available by the concerned individual. In other words, the exception does not apply merely because an individual is in a public area. Rosenthal states that an individual usually assumes that they are not known and therefore not identifiable to other people when moving in a public area, which is why the information is no personal data from the third parties' perspective. He therefore concludes that the individual lacks the will to make this information publicly available[15]. The basis of this argument is inaccurate: even though the name of an individual may not be known to other people, a person is still clearly identifiable based on a number of other factors, such as their appearance, height, and behavior. Nevertheless, Rosenthal's conclusion is correct that individuals do not have the will to make their information publicly available just by moving in a public area. Any differing interpretation would mean that personal data collected in public areas could be processed irrespective of any data protection principles.

Even if there is a violation of the data protection principles (and thus the general right of personality), such violation may still be justified according to Article 31 of the revDPA by an informed consent of the data subject, overriding interests, or the law.

- **Consent**: The consent is only valid if given voluntarily and based on adequate information for a specific processing of personal data (informed consent; cf. Article 6 Paragraph 6 of the revDPA). In case of doubt, it is the data controller's duty to prove that consent has been obtained. It is therefore advisable to obtain consent in a verifiable form (e.g., not just orally) to avoid any problems of evidence.

- **Overriding private or public interests**: The justification by overriding interests requires a weighing of interests and it is therefore oftentimes difficult to foresee the outcome in case of a dispute, as the assessment heavily depends on the judge. The assessment consists of four steps: (1) The actual private and public interests have to be determined. Private interests may not only include the interests of the data controller but also other private interests (for example the data subject's interests)[16]. "Public interest" is a term that is not really defined and is therefore open to interpretation. (2) The interests must be legitimate and worthy of protection in a legal sense. (3) The interests of the concerned individuals to have their personality rights protected must be determined.

15 HK-Rosenthal/Jöhri, DSG 12 N 57.
16 In Article 31 Paragraph 2 revDPA, the law specifies certain specific cases that may be considered to be an overriding private interest of the data controller. However, a weighing of interests is required in any case.

(4) The private and public interests for the data processing are weighed against the concerned individuals' interests. In order to serve as a justification, these private and public interests have to override the interests of the concerned individual(s).

– **Law**: This justification can be invoked if the violation of personality rights caused by the data processing in question is demanded, declared to be permitted, or implicitly presupposed by a legal provision or an official or professional duty[17]. It is therefore not sufficient that the law requires the processing of personal data in itself. The law must be specific and be linked to the violation of personality rights caused by the data processing.

In the Google Street View case, the grounds of justification played a major role because the Swiss Federal Supreme Court found the data protection principles to be infringed. As there was no consent by the concerned individuals and no legal obligation to run the service, Google had to rely on overriding private and public interests.

Google's private interests were mainly economic interests. In addition, the Federal Supreme Court (in deviation of the previous instance court) decided that Google may also invoke public interests to justify their service. The court found that Google's service was useful to a wide user base as it allows a major part of the population to find information about the public space, for example for travel planning, to find real estate, or to discover previously unknown places[18]. The question was whether these interests were adequate to justify the violation of the right of privacy and the right to one's own image of the depicted individuals or of the individuals whose house, apartment, garden, or vehicle appear on the images.

16

The court based its weighing of interests on the finding that the scope of assessment shall not only be limited to the sensitive cases, i.e. to images that depict individuals that are still recognizable. Instead, the service as a whole should be taken into consideration.

The court concluded that most images available on Street View did not contain personal data, assuming that Google's automated anonymization techniques have a margin of error of around 1 % at the time of the decision. With regard to the remaining images, it found that the personality rights of individuals are not affected to a high degree (for example if the face is not blurred but the individual is not facing the camera and thus not instantly recognizable, especially outside of sensitive areas) which is why it will be sufficient to provide a mechanism to blur/erase the relevant image data.

Furthermore, the court assumed that Google would further improve the mechanisms, based on the fact that a failure to fully anonymize the published images would bear a risk of lawsuits by concerned individuals. Based on these assumptions, it ultimately concluded that the failures to meet the data protection principles could be justified by these private and public interests.

b) Processing by Public Bodies

If personal data is processed by a public body, such as the EPFL, the data protection principles always have to be followed. The justification grounds that may apply to private entities may not be invoked by public bodies.

In addition, as already mentioned, public bodies always require a legal basis to process personal data (Article 34 of the revDPA). While disclosure is considered to be an action covered by the term "processing", disclosure of personal data by public bodies requires an explicit legal basis (cf. Article 36 of the revDPA).

A legal basis for the processing and/or disclosure may often be found in the laws that outline the purposes and functioning of a specific public body. For the processing of data by EPFL, the processing of personal data is governed by Article 36c to 36e of the Federal Act on the Federal Institutes of Technology (cf. Section IV for more details).

17 HK-Rosenthal/Jöhri, DSG 13 N 24.
18 BGE 138 II 346, Consid. 10.6.1.

2. EU

In the EU, there is no distinction between private entities and public bodies and the same principles and legal grounds apply in both cases. The processing of personal data is only lawful, if one of the following legal grounds applies (Article 6 of the GDPR):

- **Consent**: The data subject has clearly stated that he or she consents to the processing of personal data for a specific purpose.
- **Contract**: The data subject has taken steps to enter in a contract with a data controller and the processing is necessary to establish such a contractual relationship.
- **Legal obligation**: There is a legal obligation of the data controller to process the personal data in question (e.g., based on safety regulation, compliance with bookkeeping requirements).
- **Vital interests**: There are vital interests at play and the processing is necessary to protect those interests (e.g., protecting someone's life).
- **Public task**: The processing is necessary to perform a task in the public interest or for official functions that are clearly defined within the law.
- **Legitimate interests**: The processing is necessary for legitimate interests of the data controller or a third party, yet only as long as there are no overriding interests of the data subjects affected by the personal data processing. This legal ground may not be invoked by public bodies.

With regard to the potential scenarios in the context of the ScanVan project, the processing based on a public task is considered to be the most relevant legal ground: Key is that the data processing is necessary and proportional to fulfill such a public task. If equally suitable but milder means are available to achieve a public task the processing is not proportional. Moreover, the public task must be defined by a legal provision.

When private entities map cities they might be able to rely on the legal ground of legitimate interests. The term legitimate interests can be understood broadly to include commercial interests (e.g., processing for research purposes, incl. marketing research, or marketing purposes)[19]. Yet, legitimate interests alone do not suffice to legitimize the processing of personal data. The interests must be "acceptable under the law"[20], sufficiently clearly articulated, and represent a present and real interest. In addition, the processing must be necessary to achieve the pursued purpose and not override the data subject's fundamental right to privacy and data protection. Hence, this legal ground requires a three-fold testing-scheme: First, a legitimate interest must be established, second the adequacy and necessity of the processing to achieve a purpose must be established, and finally, competing interests of data subject(s) and data controller(s) must be weighed against each other[21].

F. Data Processing for Scientific Purposes

Both the revDPA (Article 39) and the GDPR (Article 89) provide certain privileges with regard to data processing for scientific purposes. We assume that the EPFL has no intention to further develop the ScanVan project using data collected in the EU and we are not aware of any scenario in which the GDPR could be directly applicable to the EPFL. Therefore, we will not analyze the scope of Article 89 of the GDPR and instead concentrate on the revDPA.

19 Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 25.
20 Ibid., 25.
21 Kamara Irene/De Hert Paul, Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach, Brussels Privacy Hub Working Paper, Vol. 4, No. 12, August 2018, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228369>, 12 ff.; Eike Michael Frenzel, in: Paal/Pauly (eds.), DS-GVO BDSG Kommentar, 2nd edition, 2018, GDPR 6 N 27 ff.

If personal data is processed by public bodies for the purposes of research, planning, or statistics, there are certain facilitations with regard to the requirements. The privileges of Article 39 of the revDPA apply if

– the data is anonymized as soon as the purpose allows it;

– the public body only discloses sensitive personal data in a manner that does not allow an identification of the data subjects;

– the recipient of the disclosed data only discloses the data to third parties with the consent of the public body that disclosed the data in the first place;

– the results are published in a manner that does not allow an identification of the data subjects.

If all of these requirements are met, the principles of transparency and purpose limitation do not apply[22].

In order to benefit from the research exemption, it is key that the collected raw image data is anonymized as soon as possible, depending on the purpose. If the original image data is necessary for the purpose of training the anonymization process or enhancing photogrammetry methods, it may be kept as long as it serves these purposes. In any case, the results of the project may only be published in a manner that does not allow an identification of any data subject.

G. Data Subject Rights

1. Legal Requirements

If personal data is processed, the concerned individual may exercise the following data subject rights with the data controller (or processor):

revDPA (CH)	GDPR (EU)
right to be informed (Articles 25 ff.)	right to be informed (Articles 13 f.)
right of access (Articles 25 ff.)	right of access (Article 15)
right to rectification (Article 32 Para. 1)	right to rectification (Article 16)
right to erasure (Article 32 Para. 2 lit. c)	right to erasure (Article 17)
–	right to restrict processing (Article 18)
–	right to data portability (Article 20)
right to object (Article 32 Para. 2 lit. a & b)	right to object (Article 21)
rights related to automated decision making (ADM) and profiling (Article 21)	rights related to automated decision making (ADM) and profiling (Article 22)

The ScanVan project collects personal data only as an undesired side-product and it will therefore be relatively straight-forward to comply with requests of data subjects in most cases.

– **Right to be informed**: Data subjects have the right to be informed about what personal data concerning them is processed, as well as the means and purposes of the processing.

– **Right of access**: Data subjects may request access to the personal data concerning them.

– **Right to rectification**: In case personal data is inaccurate, data subjects may request the data to be rectified.

– **Right to erasure**: Data subjects may request that their personal data is erased.

22 Furthermore, there is no need to fulfill the stricter requirements with regard to the legal basis in case sensitive personal data is processed and there is no need for a legal basis for the disclosure of the data.

– **Right to restrict processing**: Data subjects have the right to request the restriction of processing of their personal data.

– **Right to data portability**: Individuals may request a copy of their personal data in order to reuse it for their own purposes on a different service without affecting its usability. This right has to be seen in the context of making sure that people may switch to another service provider.

– **Right to object**: Data subjects have the right to object the processing of their personal data.

From a design perspective, it must be made sure that data subjects may submit their requests in an easy way. Having said that, it must be noted that most of these data subject rights are not absolute and only apply in certain circumstances. In case of such a request, the situation should therefore be analyzed by a data protection expert, also because data controllers have a limited timeframe to react for individual rights request (e.g. the data subject should, in principle, be able to obtain access to their data within a month).

In case the GDPR is applicable, the data subjects will have to be informed about their data subject rights (cf. Article 13 Paragraph 2 of the GDPR). This information is usually provided in a privacy policy (cf. Section III.D.2).

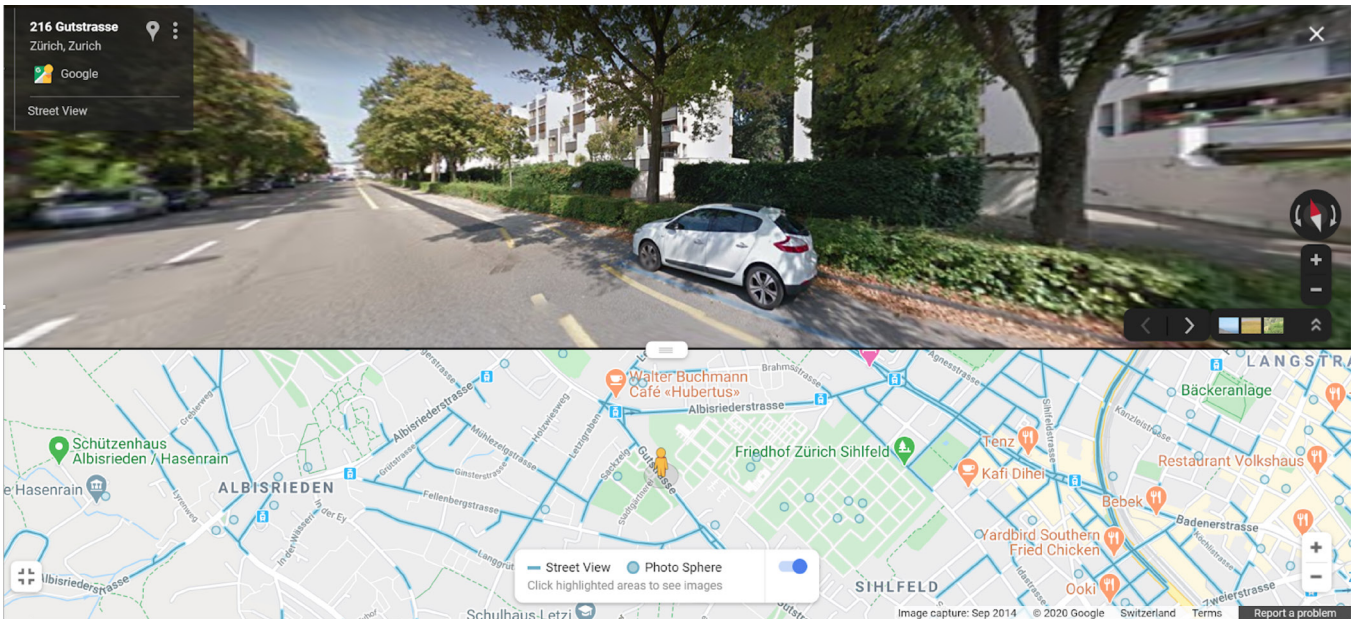
2. Recommended Actions and Design Considerations

In the ScanVan case, due to the fact that the depicted individuals are not known by name, several difficulties arise in connection with the data subject rights:

First, difficulties may arise in connection with the verification of requests because it must be made sure that the individual submitting the request indeed is the individual depicted on a specific image or at a specific location in the 3D point cloud. If such a request concerns the erasure of personal data, it is advisable to comply with the request irrespective of who submitted it. In this case, irrespective of whether the right individual filed the request, this will be in compliance with data protection laws and will help to avoid future requests by other individuals. However, a verification of the individual submitting the request is required in case of other subject rights, especially if it involves disclosure of data that is not yet publicly available. In these cases, it might be necessary to request a copy of an identity document to make sure that personal data is not disclosed to any unauthorized third party.

Furthermore, problems may arise in case only the 3D point cloud is published, and the original image data is not deleted. In this case, from the perspective of the data controller (or processor), individuals in the 3D point cloud (even though unrecognizable by the 3D point cloud itself) may still be identified by looking at the image data. Concerned individuals may therefore argue that the 3D point cloud is personal data and that the data subject rights therefore also apply to the 3D point cloud. If a concerned individual requested the erasure of their data, compliance with this request could be achieved by anonymizing the original image data (no erasure of the 3D point cloud is required). However, in practice, these cases will be rather unlikely because individuals will not recognize themselves in the published 3D point cloud and will therefore be reluctant to submit any requests.

In addition, it might be advisable to provide a possibility for concerned individuals to make reference to a specific area of the image data or 3D point cloud in order to efficiently handle requests with regard to data subject rights. This might be achieved by providing an online form on the website where specific areas may be tagged, similar to the reporting function that is implemented on Google Maps:



Why are you reporting this image? (Please choose from one set of options.)

Request blurring: What would you like us to blur?

- ○ A face
- ○ My home
- ○ My car / a license plate
- ○ A different object

Implementing a specific online form to submit requests in connection with data subject rights is not a legal requirement, as data subject rights may also be exercised by other means of communication, such as e-mail, letter, or phone. As it may be complex and expensive to provide a specific online form, it should therefore be taken into consideration whether this initial effort makes sense compared to the expected number of filed requests and the time saving this online form provides in these cases. The implementation of a reporting tool that is easy to use for concerned individuals also plays a major role with regard to the principle of proportionality (cf. Section III.D.3) and as a ground of justification (cf. Section III.E). If the image data shall be published, it is therefore highly recommended to implement such a reporting tool.

However, if only the (anonymized) 3D point cloud is published online, such a reporting tool will most probably not be required because individuals do not even recognize themselves and the likelihood of any requests to exercise their data subject right is therefore relatively small. Even if only the 3D point cloud is published, if the GDPR is applicable, it would still be necessary to mention the data subject rights in a privacy policy.

IV. Publication of Image Data and 3D Point Cloud of Sion by EPFL

This section provides a specific analysis of the following scenario: The EPFL project team collects image data of the city of Sion and generates a 3D point cloud thereof. Both the original image data and the 3D point cloud of Sion are published through a web-based application online. Anyone worldwide can access the image data and the 3D point clouds.

A. Legal Basis for Processing and Publication

The EPFL is one of the two Swiss federal institutes of technology and fulfills the purposes specified in Article 2 of the Federal Act on the Federal Institutes of Technology (ETH-Act). From a data protection perspective, the EPFL is a public body (Article 5 lit. i of the revDPA) and therefore requires a legal basis for the processing and disclosure of personal data (cf. Section III.E.1).

Article 36c of the ETH-Act states that personal data may be processed by the EPFL within the scope of research projects, to the extent that such processing is required for a specific research project. This provision, however, does not mention the disclosure of personal data and it is questionable whether it would meet the requirements of Article 36 of the revDPA. According to the ETH-Act, it is the federal institutes' purpose, i.a., to expand scientific knowledge through research and to ensure a dialogue with the public (Article 2 Paragraph 1 lit. b and e), which might support the view that personal data may also be disclosed to the public. However, the restrictive wording of Article 36c (insofar as required for given research project) seems to limit disclosure of personal data for the purpose of the ScanVan project.

The purpose of the ScanVan research project is to generate 3D point clouds of the architecture of cities. While we would not rule out that the publication of the 3D point clouds might fall within the legal basis provided in the ETH-Act, this question may be left open because the 3D point clouds by themselves (to the extent they are not combined with the original image data) are not considered to be personal data. However, the publication of the original image data seems to be difficult to justify because this does not seem to be strictly required for the ScanVan project. If the original image data shall help to understand how the 3D point clouds are generated, it would be sufficient to only publish certain images where it was made sure that they are completely anonymized. We would therefore argue that the publication of the entire image data including personal data would not be covered by Article 36c of the ETH-Act and the **publication of original image data must therefore be avoided, unless a prior full anonymization is ensured**. Any design recommendations discussed in the following with regard to the publication of the original image data (unless fully anonymized) may potentially reduce the severity of the violation of personality. However, these measures are no substitute for a legal basis and do not render such publication lawful.

B. Data Processing for Scientific Purposes

If only the 3D point cloud is published, the requirements of Article 39 of the revDPA should be met because no personal data is published. This means that the principles of transparency and purpose limitation do not have to be followed.

However, Article 36e of the ETH-Act stipulates an additional obligation to inform the data subjects, which basically corresponds to the principle of transparency. In other words, even though the research exemption applies, the transparency still has to be ensured.

C. Data Protection Principles

1. Lawfulness

In order to generate the 3D point clouds, a significant number of images were taken in Sion without any consent of the concerned individuals or even without their knowledge, which might impair the right to their own image. Nevertheless, contrary to the Google Street View case, these images will not be published online. Unlike in the context of data protection law, where a violation does not require a particular severity, the impairment of the general right of personality must reach a certain intensity to be legally relevant. As such, not every impairment of the personality constitutes a violation of the general right of personality. With regard to the right to one's own image, no violation is usually assumed if an individual only appears as staffage and is not the primary subject matter of the image[23]. However, in the Google Street View case, the Federal Supreme Court decided that the depicted individuals are not only staffage and that there is a violation of the right to one's own image, arguing that the focus of attention may ultimately be chosen by the user (e.g., by zooming). This argument may not be directly applied to the 3D point cloud of Sion because the image data is not available to the user. It might therefore be questioned whether the right to one's own image of these individuals is indeed violated in the present case.

If the right to one's own image is considered to be violated, this violation would have to be justified in order to make the capturing and usage of these images lawful. In this scenario, the image data is only an interim step that is not desired but absolutely necessary to generate the 3D point clouds. As the images are not captured to draw any conclusions about the depicted individuals, the harm that is caused to the concerned individuals is not very severe. On the other hand, the research that is enabled through these images is important for the EPFL to fulfill the purpose according to the ETH-Act and to advance science. Given that the project is in line with the purpose of the ETH-Act as a federal law, it may without doubt be assumed that this research serves the society as a whole.

As a result, it may be assumed that there are overriding public interests that justify the relatively small infringement of the concerned individuals' right to their own image. The principle of lawfulness is therefore fulfilled (as long as the original image data is not published).

2. Transparency

To the extent personal data is processed for scientific purposes, the principle of purpose limitation and transparency according to Article 6 Paragraph 3 of the revDPA is not applicable (cf. Section IV.B). However, as already mentioned, Article 36e Paragraph 1 of the ETH-Act states that the EPFL is "required to inform the persons affected regarding the collection and processing of personal data in connection with a specific research project".

The EPFL has no possibility to directly contact the individuals depicted in the original image data. The information duty would therefore have to be fulfilled by public communication over the website as well as through local media (e.g., Le Nouvelliste).

Having said that, it is questionable whether such information is recommended in practice, as the collection of the image data was conducted some time ago. If the (anonymized) 3D point cloud is published without any public communication, the risk that someone would complain about non-compliance with the ETH-Act would probably be relatively small. If, however, information is published in the media, this might rather increase than mitigate the risk of complaints (even if they are legally unfounded).

3. Other Principles

With regard to the principle of proportionality, it may be stated that the image data is suitable and necessary to generate 3D point clouds and to conduct research in this regard. Furthermore, as already stated in the context of the right to one's own image, the personal data is only an undesired side-product and in no way analyzed in connection

23 BSK ZGB I-Meili, ZGB 28 N 20.

with the concerned individuals. The harm that is caused to the concerned individuals is therefore minimal. On the other hand, the benefits of the 3D point clouds and especially the research conducted with regard to the technology are substantial. It may therefore be assumed that the principle of proportionality is fulfilled as long as no personal data is published.

The EPFL intends to keep the original image data in order to be able to further improve the photogrammetry process and to generate more accurate 3D point clouds in the future without having to scan the entire city a second time. As the image data still serves the same research purpose and for as long as the development of the technology is ongoing, this retention of the image data is in line with the principles of data minimization and storage limitation.

As the data is processed for scientific purposes and fulfills Article 39 of the revDPA (unless the original image data is published), the principle of purpose limitation does not apply. This means that the original image data may in principle also be used for other research projects. In this case, however, the new project would also have to be assessed from a data protection perspective.

No problems should occur in connection with the principle of accuracy (cf. Section III.D.4). It must be ensured that appropriate data security measures are implemented and that these measures are documented (cf. Section III.D.5).

D. Data Subject Rights

If only the 3D point cloud is published, it is rather unlikely that there will be many requests of individuals to exercise their data subject rights (cf. Section III.G.2). Nevertheless, the website should contain certain contact details in the imprint or in the privacy policy that allow concerned individuals to contact the EPFL.

E. Potential Consequences of Non-Compliance

In case of non-compliance with the data protection regulations, the EPFL may face two different types of legal procedures:

– Investigation and measures by the Federal Data Protection and Information Commissioner (FDPIC)

– Complaints and/or legal actions by anyone with an interest to warrant protection (i.e. mainly the concerned data subjects)

These legal procedures may be initiated independently from each other and may also lead to different outcomes.

1. Investigation and Measures by the Federal Data Protection and Information Commissioner (FDPIC)

The FDPIC may initiate an investigation if there are sufficient indications that a data processing could violate the data protection regulations (Article 49 of the revDPA). In case of an investigation, the public body is obliged to cooperate and to provide information to the FDPIC (cf. Article 49 Paragraph 3 and Article 50 of the revDPA).

If the FDPIC finds an infringement of the data protection regulations, the FDPIC may, i.a., order that the data processing is adjusted, suspended, or terminated and that the personal data is fully or partially deleted or destroyed (Article 51 Paragraph 1 of the revDPA). The FDPIC may also decide to stop the investigation without issuing an order and to only issue a warning in case the public body takes the necessary measures to restore compliance with the data protection regulations.

If the FDPIC issues an order, the concerned public body may either implement it or challenge it in a procedure before the Federal Administrative Court (cf. Article 35 lit. b of the Federal Administrative Court Act). This court decision can then be appealed to the Federal Supreme Court.

If the EPFL were to publish the original image data without sufficient anonymization, it may not be excluded that an investigation is opened if the FDPIC becomes aware of the project (either by himself or upon notice by the public). Having said that, the general public today may already be quite used to similar image capturing processes such as Google's Street View and the risk for complaints may therefore be somewhat smaller. Especially if the EPFL upholds the data protection regulations at least to the standards of these other actors, it may take a while until the FDPIC is urged to take a closer look. If, however, an investigation is opened, this would probably put an end to making the original image data available online. Besides the legal effects, the fact that such an investigation is carried out alone may of course also lead to reputational damage. As stated, these risks may be avoided by ensuring a full anonymization of the images.

2. Private complaints and legal actions

In case data is processed by public bodies, anyone with an interest to warrant protection (usually only the data subjects) may demand that the responsible public body

- refrains from unlawfully processing personal data (Article 41 Paragraph 1 lit. a of the revDPA)
- removes the consequences of unlawful processing (Article 41 Paragraph 1 lit. b of the revDPA)
- ascertains the unlawfulness of the processing (Article 41 Paragraph 1 lit. c of the revDPA)
- corrects personal data (Article 41 Paragraph 2 lit. a of the revDPA)
- deletes or destroys the personal data (Article 41 Paragraph 2 lit. a of the revDPA)

The public body will have to issue an order in which these demands have to be addressed. The order may then be challenged by the data subject by filing a lawsuit with the Federal Administrative Court.

In addition, the data subject may file a claim for damages and satisfaction according to Article 28a Paragraph 3 of the Civil Code. In the data protection context, it will often be very difficult for the data subject to show that there have been any damages (meaning a negative impact on their assets, either by a decline of assets or an increase in liabilities) as a direct consequence of the unlawful data processing. Satisfaction, on the other hand, may be awarded without any financial loss in case the violation of the personality rights reaches a certain severity (cf. Article 49 of the Code of Obligations and Article 6 Paragraph 2 of the Federal Accountability Act).

If the original image data is published by the EPFL without sufficient anonymization, it is possible that a data subject may demand satisfaction, for example if they are depicted in an unfavorable way or in a context that sheds a negative light on them. As mentioned, damages will be quite difficult to prove, and such claims are therefore rather unlikely. In addition, claims for damages and satisfaction pose a significant financial risk to the claimant (costs for an attorney, court fees, etc.). Therefore, rather than initiating legal proceedings, it is likely that concerned data subject will first contact the EPFL directly to find a solution. It may be expected that in many cases, deleting the respective personal data and offering a sincere apology will be sufficient to avoid any further consequences.

F. Conclusions

In order to generate the 3D point cloud, the EPFL relies on image data collected in Sion that contains personal data. It must therefore be ensured that the transparency obligation according to the ETH-Act is fulfilled. In order to fulfill this obligation, the website that contains the final 3D point cloud should contain a privacy policy in compliance with applicable data protection laws (cf. Section III.D.2).

If the transparency obligation is fulfilled, the generation and publication of the 3D point cloud should be in compliance with all legal requirements. The retention of the original image data is also allowed as long as this data is required for the further development of the technology.

However, the publication of the original image data must be avoided in order to ensure legal compliance. There is no legal basis for such a publication of personal data, the publication is unlikely to be proportional, and the general right of personality of the concerned individuals would be infringed without sufficient grounds of justification. Non-compliance with the data protection regulations may result in an investigation by the FDPIC and ultimately a ban to publish the original image data. Even though the risk of such a lawsuit is small, claims for damages and satisfaction by concerned data subjects are possible. To avoid these risks, it must be ensured that any image data is anonymized before publication.

Imprint

Center for Information Technology,
Society, and Law (ITSL)
University of Zurich
Raemistrasse 74|38
8001 Zurich
Switzerland