Facial recognition

Privacy considerations in access control

The use of facial recognition is increasingly used for physical access control. Using this technique comes – inevitably – with the processing of biometric data and has therefore impact on people's privacy. In this paper privacy aspects that need to be taken into account when using this type of technology are discussed as well as the tools to get started with facial recognition software for your business.

Facial recognition technology

An algorithm is used to filter a human face from a video or photographic image. In only a few milliseconds, the face's characteristics are recorded and converted into a unique code. Then the facial recognition software compares the code to a database. If it finds a match, this can be used to identify the individual in the image and determine whether or not to provide access.

One of the major advantages of facial recognition access control is the lack of waiting at the access point. The software will register a person's face as they approach and can determine whether to allow access in the time needed to arrive at the gate. When the authorized person is near or at the access point, the system opens the gate. This prevents unauthorized individuals from slipping through the open gate. Also, the person can proceed smoothly through the access point.

Privacy aspects to consider

An example where the processing facial recognition technology is used to identify, authenticate and verify an individual. In this context of processing, the General Data Protection Regulation (GDPR) applies.

In order to implement facial recognition in your access control system successfully and in compliance with the GDPR, specific aspects need to be considered:

— Lawful basis
— Consent
— Transparency
— Purpose Limitation
— Privacy Impact Assessment
— Data retention
— Data minimization
— Security measures

These aspects will be further explained in this paper.

Use of biometric data

When implementing facial recognition access control, several GDPR related principles need to be adhered to. In this section we focus on what is required.

Lawful basis

Facial recognition makes use of biometric data. According to The General Data Protection Regulation (GDPR), biometric data is a special category of personal data (also called sensitive data). In principle, it is prohibited to process sensitive data, unless an exception applies. A possible exception can be **explicit consent** of the data subject or if it is **necessary for authentication or security purposes**. An important public interest must be involved to meet the latter requirement.

An example where the processing of biometric data is necessary for authentication or security purposes is the security of a nuclear power plant. In this case, the public interest is of great importance and only a select and vetted group is allowed access. According to the Dutch DPA, the importance of security for e.g. a recreational area, the garage of a repair shop, or a supermarket is not so significant that it merits the use of biometric data for access.

The question whether there is an important public interest will depend on the specific circumstances, but in general this will only apply to specific and limited situations. Therefore, in most cases, consent will be the only legal basis for the processing of biometric data.

Consent

Consent in the sense of GDPR means any *"freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*
For explicit consent it means simply stated: the data subject should quite literally and explicitly say "I consent" for consent to be considered explicit.

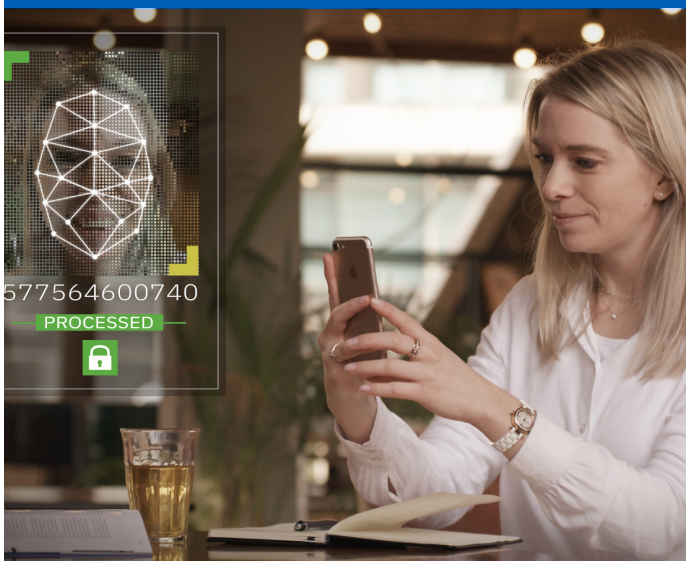
For consent in an employer-employee relationship it cannot be assumed that consent automatically follows this relationship.

Within this relationship there is a hierarchy and therefore consent may not always be 'freely' given. It is therefore crucial that consent is **freely given** by offering an alternative (access by card) that does not pose any disadvantages for the data subject.

We would like to emphasize that, in almost all cases, consent will be the only possible lawful basis. Consent in the context of an employer-employee relationship can be a grey area. This means as a minimum, the following must be considered:

- Consent must always be given freely (the employee needs to have a choice).
- Data subjects are not and will not be disadvantaged in any way by not giving consent.
- Consent can be withdrawn at any time.
- The data subjects concerned are well informed and know what they are giving consent for.
- The consent is demonstrable.
- The data subjects must demonstrate consent by means of a clear affirmative action.

Engage with your legal counsel how and under what conditions you can use permission for this solution.



Transparency

Data subjects must be informed adequately about the processing of their data. This information must be provided at the time when personal data are obtained or before the consent is given. At the entrance / access control entry, data subjects must be informed via, for example, a sign. The data subjects who are not subject to the access control system and have not given consent may also be, or assume that they are being, filmed. It is therefore wise to also direct the information to them. Articles 13 and 14 of the GDRP describe the requirements for the information provisioning.

Purpose limitation

Personal data must be collected for a predetermined specified, explicit and legitimate purpose. Be aware that the personal data may not be used for other purposes. It is not allowed to use the data at a later moment for purposes such as: checking who has been at the office at what time or to monitor the number of people in the office for security or health purposes. See the next page for more information on how Boon Edam's facial recognition software can assist.

Privacy Impact Assessment

The processing of biometric data in the context of access control is not without risks and therefore a Privacy Impact Assessment must be performed. This document must, among other things, take into consideration the various interests, including those of the data subjects involved. In addition, the lawful basis for processing and the risks associated with the processing of biometric data must be assessed. When performing the assessment, the security measures already taken by the software need to be taken into account.

When implementing facial recognition access control, several GDPR related principles need to be adhered to. In this section, we discuss the more technical principles that may or may not be incorporated in the software of the facial recognition system already. Keep in mind that processing limitation, security measures, data minimization and data retention of personal data should be demonstrable and can be supported by the system or software itself.

Processing limitation

According to the GDPR, organizations must ensure that only data for which there is a legal basis for processing is processed and only to the extent that is required to fulfill the purpose. In other words: personal data of people who do not want access through facial recognition are not used or stored. The purpose for processing should be predefined and documented. Note that some providers offer technical solutions for not processing data of individuals that are not in the database of the access control system.

Security measures

Technical measures should be incorporated in the system to protect personal data and to ensure its integrity, confidentiality and availability, for example, encryption, password protection and spoof detection. Next to that, your organization should asses what other organizational and technical measures should be taken.

Data minimization

Data collection must be relevant and limited to fulfill the purpose. For example, the access control system should only process the unique mathematical code based on an image of a person in another database or system, not images itself or any other related personal data. Note that in line with purpose limitation, the system should not store data around who had access to the office at what time or who tried to get access to the office.

Data retention

In order to store data for the shortest time possible, the access control system must ensure that data is deleted once it is no longer necessary. For example, when the check is done and someone has been granted access, no data should be stored. Next to that, your organization should take appropriate measures to erase data when its no longer necessary. As an example, your organization should delete the data in the access control system or in the source system when an employee leaves the organization.

Example

Facial Recognition in Access Control

We see that in the marketplace the technical solution providers for facial recognition software provide options and features to facilitate data processing safeguards. In this section we outline an example of such a technology and provide insights in how similar technologies can be used in your organization to safely and securely implement a facial recognition access control setup.

Anyvision is one of those solution providers that have built-in privacy features and modes to facilitate your organization to comply with GDPR standards and more specific in the technical measures as outlined above. Anyvision is offering its solution in conjunction with the access control solutions from Boon Edam, which makes the example very illustrative for this case. The anyvision software is directly connected to the access control door or tourniquet and provide access to individuals that have a matching profile in the facial recognition database. The software provides the option to enable the built-in privacy mode. With this mode enabled, the backend only stores mathematical code based on an image of an enrolled individual and not any images in itself. Individuals that pass the facial recognition camera's who are not enrolled in the database are only matched with the database to validate access. After that, the mathematical code of the individual will no longer be present. Only the mathematical code will be compared. This will provide the end-user with technical measures to comply with data minimization and data retention requirements.

Furthermore, the front-end has a built-in face-blur mode, which contain several features with the purpose of mitigating the risks for the data subjects involved. With the this mode activated, the front-end system will use face-blur techniques to ensure that video images of individuals passing the system are not shown in the front-end. This way, the personal data that is not necessary will not be processed. Also, in this mode it is not possible to generate reports on who entered and when. This will enable the end-user to answer for example aspects of the purpose limitation of the GDPR.

Please bare in mind that although different technical measures might be included to mitigate any privacy related risks, an organization must always make an evaluation if the risks are efficiently mitigated and to balance interest.

Privacy Checklist

The publication of this paper is to provide clear information which privacy aspects should be taken into account when implementing facial recognition as access control for your organization. Below, an overview of the fundamental principles of what your organization must do and where KPMG and the Facial Recognition software can assist:

01 **Lawful basis**
Determine a lawful basis for processing biometric data and document this.

02 **Consent**
Make sure consent is justified, demonstrable, informed and freely given and record this.

03 **Transparency**
Inform data subjects properly and prior to the processing.

04 **Purpose limitation**
Process data for only predetermined, specified, explicit and legitimate purposes.

05 **Privacy Impact Assessment**
Document the processing, the risks and measures in a Privacy Impact Assessment. KPMG can assist you to conduct this assessment.

06 **Processing limitation**
Process data for access control only and not for other purposes. Make sure to document this in the PIA and to enable the privacy feature.

07 **Data retention**
Delete data as soon as possible, preferably right after access was provided. Make sure to document this in the PIA and to enable the privacy feature.

08 **Data minimization**
Process only data that is absolutely necessary for the determined purpose and document this in the PIA and to enable the privacy feature.

09 **Security measures**
Implement adequate security measures. Make sure to enable the privacy feature

Contact information

**Do you want more information on how we can help your organization?
Feel free to contact us.**

Koos Wolters

Partner Data Privacy
T +31 6 5333 7486
E wolters.koos@kpmg.nl

Stephan Idema

Senior Manager Data Privacy
T +31 6 5275 5924
E idema.stephan@kpmg.nl

home.kpmg/nl/dataprivacy