essentry

Digital Visitor Management with Biometric Identity Verification

Evaluation, requirements and guidelines for
a legally compliant introduction

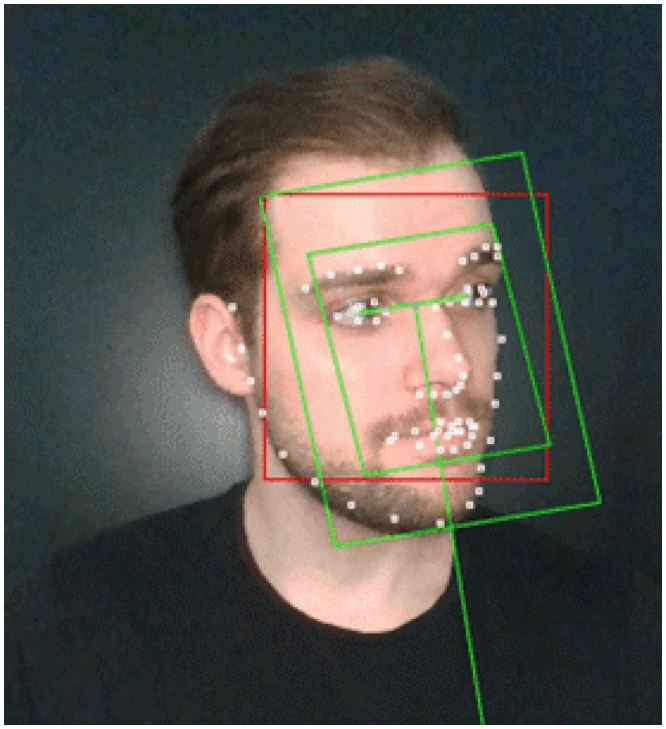
1. Introduction

Physical building security is becoming increasingly important in times of ever more sophisticated security attacks on companies. The visitor management process plays a decisive role in this. This is because effective visitor management ensures that only authorised persons are granted access to company buildings.

The so-called "Storming of the US Capitol" in January 2021 demonstrated the far-reaching consequences that uncontrolled access to buildings can have. Not only must the physical damage be repaired as a result of the incident, but all computers and rooms must also be considered compromised. Questions arise such as „Were listening devices placed in the MPs' offices?", „Were USB sticks used to download data from computers, or to place „backdoors" that would allow subsequent unauthorised remote access?". All of this needs to be investigated in the aftermath and all inventory needs to be examined, replaced or refurbished.

Manual visitor management processes, which have to meet high security requirements, are cost-intensive and involve time-consuming, tedious registration, authentication and approval steps for all persons involved (visitors, hosts, security staff). Digital visitor management systems provide a remedy here. With the right system, security can be significantly increased, process efficiency enhanced, and the user experience improved at the same time.

Modern visitor management systems enable a largely automated, highly secure access process for visitors. This is made possible by biometric identity verification combined with integration into existing access control systems. With automated identity verification, biometric features such as the face are compared with a reference such as an identity document that has been checked for authenticity. The resulting increased physical security must be combined with a sophisticated data security and data protection concept, because the collected data are particularly worthy of protection. Within the EU, the processing of biometric data is clearly regulated in the General Data Protection Regulation (GDPR). In this white paper, we explain the requirements for a GDPR-compliant use of digital visitor management systems in which biometric data are processed (hereinafter also referred to as biometric visitor management system).



1:1 Face recognition

2. Biometric data and GDPR

The processing of biometric data is data pursuant to Article 9 of the GDPR. This article also regulates the conditions under which biometric data can be processed. In addition to the GDPR, European and German data protection authorities have dealt with the processing of biometric data in detail, both individually and jointly via the Conference of Independent Data Protection Authorities of the Federation and the Länder (DSK). In this white paper, we rely, among others, on the information contained in „Guidelines on Facial Recognition" 1 of the European Data Protection Convention, „Position Paper on Biometric Analysis" 2 of the DSK, as well as the statement on „Biometrics and Data Protection" 3 of the Federal Data Protection Commissioner.

The following sections outline the requirements that must be met in order to ensure the legally compliant introduction of a biometric visitor management system, based in particular on the aforementioned sources.

1 https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3
2 https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/
3 https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/BiometrieUndDatenschutz.html

3. Legal bases

Biometric data may be processed if there is an applicable permission as defined in Art. 9 (2) of the GDPR. This article lists the possible permissions. The permission relevant to the context of biometric visitor management systems (consent and legitimate interest) are described below.

3.1. Consent

The primary legal basis is obtaining consent from the data subjects (customers, visitors, employees) pursuant to Art. 6 para. 1 lit. a GDPR.

In order for the consent to be legally effective, the requirements of Art. 7 of the GDPR must be met. In particular, consent must be given voluntarily and the data subject must be informed about the essential points of the data processing.

In order to meet the requirement of voluntary consent, the visitor must be given the choice of whether to give consent or not. In the event of not giving consent, the visitor (i.e. the data subject) must not suffer any disadvantages. In practice, this must be ensured by providing an alternative access process, for example through a manned reception or a manual identity confirmation by the host when collecting the guests in the reception area of the building.

3.2. Legitimate Interest

In individual cases, the legitimate interest pursuant to Article 6 (1) sentence 1 lit. f GDPR may be considered as a further legal basis in combination with a circumstance pursuant to Article 9 (2) GDPR and a necessity test.

3.2.1. Permissibility

There are two circumstances that may be applicable in the case of a biometric visitor management system:

- Art. 9 Abs. 2 lit. g GDPR: **Substantial public interest**: For example, there is a public interest in the security of critical infrastructures (for society). This includes airports, the food industry, the chemical industry, the energy sector and data centre operators. As a basis for Art. 9 (2) (g) GDPR, a legal ground of EU law or the law of a European member state is required. For example, an airport operator can refer to Section 8 (1) No. 4 of the Aviation Security Act; according to this, the operator of an airport is obliged to protect operations from attacks and unauthorised access.
- Art. 9 Abs. 2 lit. f GDPR: processing is necessary for the **establishment, exercise or defence of legal claims.** Here, there is considerably more freedom with regard to the argumentation, as it depends strongly on the necessity test and a credibly presented danger of possible (unjustified) legal claims has to be argued.

3.2.2. Necessity test

In order to invoke legitimate interest, a necessity test must be carried out in addition to the existence of one of the aforementioned permissible circumstances. As a result, the data processing must be necessary to protect legitimate interests and the interests of the data subject must not be compromised. The check is carried out in three stages:

- demonstration of own interests
- Necessity of the data processing to safeguard these interests (Is there an equivalent, suitable and more lenient means?).
- Weighing up against the interests, fundamental rights and freedoms of the data subject in the specific individual case.

In general, the purpose should be stated as precisely as possible. In this case, the purpose is **digital visitor management** and not general visitor management.

4. Technical requirements on part of the data processor

The technical requirements for the use of biometric visitor management systems include, on the one hand, the security of the processing and, on the other hand, data privacy-friendly default settings that can be configured on the product side.

4.1. Processing security

The processor, i.e. the provider and operator of the biometric visitor management system, must be able to demonstrate suitable measures that guarantee secure data processing. These should be documented in the order processing contract. Appropriate measures include, but are not limited to:

- The provider's compliance with the GDPR is continuously monitored by an independent external data protection officer.
- All data stored is encrypted according to AES-256.
- All data is encrypted during transfer according to TLS. Between check-in kiosks and cloud system, communication should additionally be secured via VPN.
- Developers use an encrypted connection (SSH, SSL/TLS) to the systems.
- The databases are hosted in a highly secure data centre in the EU.
- The system undergoes regular penetration tests conducted by independent, specialised companies.
- The provider can demonstrate information security certification, such as ISO 27001 according to BSI IT-Grundschutz.

Biometrisches Besuchermanagementsystem

4.2. Privacy-friendly default settings

In addition to the aforementioned measures, which primarily concern the infrastructure of the product, the biometric visitor management system should have data privacy-friendly default settings. Especially when processing data from ID documents, it must be precisely documented which data is actually processed and stored. The most important aspects are listed below:

- **ID verification should always take place locally** on an end device, so that no cloud-side processing of the entire ID document takes place.
- **No image of the ID document** should be **stored locally** either, but should be deleted directly after verification.
- The system should only perform a **biometric verification**, not a *biometric identification*.
    - With *biometric verification*, the user discloses his identity to the system in advance (e.g. by scanning a QR code assigned to him) and the system then compares the biometric feature (the face) only with the one reference feature matching the user ID. This corresponds to a data-efficient 1:1 comparison.
    - In contrast, *biometric identification* compares the biometric feature with all reference features stored in the system. This corresponds to a 1:n comparison in which an arbitrarily large amount of data is processed.
- **Data deletion and retention periods** should be configurable by the customer (i.e. the controller) for the different types of data.
- The system should offer the possibility to **display data protection policies to the user** and, if necessary, to **obtain user consent** for data processing and to store it in relation to the individual.

In practice, it is often the case that by using modern digital visitor management systems, not only can the aforementioned requirements be met, but data protection is even increased compared to manual visitor management processes. The following table (Page 5) compares the typical manual process with a data protection-friendly digital process.

Typical manual process	Data privacy friendly digital process
Incomplete validation The human eye is not able to verify the authenticity of ID documents. In addition, the visitor gives his ID card out of his hand during the visual check.	✓ **Validation of the ID locally on the Check-in kiosk** (Takes 3 photos of the ID card with 3 different light sources to check that the document has all the security features). The photos of the document are deleted immediately after validation.
Manual face match Error-prone manual face matching by reception staff.	✓ **1:1 face match** This is done by comparing the photo cut out of the ID document with a selfie taken by the kiosk camera.
Manual data processing and intransparent retention periods Typically, visitor data is stored and shared across multiple systems or forms. Retention and deletion policies are often not enforced.	✓ **Allow custom view and data retention periods** The system is configurable according to the needs of the client and offers different options in the reception view (e.g. show selfie or not). User-defined retention periods / deletion rules can be individually configured for each data category.
Intransparent data privacy policies and lacking consent If at all, data protection policies are typically only presented in paper form and consents are not stored centrally or are not traceable (e.g. for audits).	✓ **Data protection and Consent** Reference (customisable) to the privacy policy at several points in the process, e.g. - Link to privacy policy in the invitation, online check-in and on the kiosk screen. - In the invitation email, it is pointed out that an identification document is required for on-site registration due to high security requirements - Customisable to additionally ask for explicit consent at online check-in or on-site at the kiosk screen.

5. Requirements for the data controller

On the part of the data controller, the following measures should be carried out before introducing the biometric visitor management system. Leading providers of biometric visitor management systems support the customer in the implementation of the measures with document templates and information.

- Data protection impact assessment
- Data processing agreement
- Information requirements / data protection declarations

DSGVO-konform

5.1. Data protection impact assessment

If innovative technologies are used, Article 35 (1) sentence 1 of the GDPR requires a data protection impact assessment to be carried out. This obligation is also included in the so-called “must list” of the supervisory authorities, according to Article 35 (4) sentence 1 of the GDPR, according to which the controller must always carry out an impact assessment when using biometric access systems. This assessment must identify foreseeable risks to the rights and freedoms of data subjects and assess the consequences of the envisaged processing operations.

The data protection impact assessment for the use of biometric visitor management systems should list basic technical risks and corresponding protective measures. In addition, the probability of occurrence of each risk should be assessed. Furthermore, customer-specific risks can be determined with the respective responsible persons in order to also include individual organisational risks in the impact assessment. The data protection risks, probabilities of occurrence & protective measures taken should be revised cyclically by the controller together with the provider of the biometric visitor management system to include legal and technical developments.

In the data protection impact assessment, it must be taken into account that - despite the high legal requirements - the use of biometric access controls has become a mass phenomenon. Technologies such as fingerprint sensors or “face unlock” are used by almost every smartphone user today.

5.2. Data processing agreement

To cover additional legal framework conditions for the use of biometric visitor management systems, corresponding

Biometric visitor management system

contracts for data processing must be concluded in accordance with Art. 28 of the GDPR. These contracts transparently regulate the rights and obligations for both the controller and the processor. The provider of the system should be able to present a contract for this purpose.

5.3. Information obligations and rights of the data subject

Data controllers must comply with their information obligations under Art. 12-14 GDPR in an easily accessible form. All rights of the data subjects as well as the recipients of the personal data are presented transparently in a privacy statement. The information obligations should be provided in the course of the registration and check-in process. Modern visitor management systems offer customers the option of adding their own data protection statements to the system in the administration interface and also support them with text templates.

It is also advisable to introduce a process for responding effectively and in a timely manner to data subjects‘ rights, such as requests for information in accordance with Article 15 of the GDPR. Leading visitor management software providers have implemented processes to support responsible bodies simply and quickly in responding to data subject requests, so that the legal deadline of 14 days can be met in any case.

6. Conclusion

As a result, the introduction of a biometric visitor management system is legally compliant if the requirements described in this white paper and any company-specific requirements are met. In this regard, there are clear regulations in the GDPR and the statements of the data protection authorities offer further implementation guidelines.

Leading visitor management system providers support their customers every step of the way and work closely with the respective legal departments or data protection officers to ensure that all requirements are met. In this way, what at first appears to be a dilemma can be solved: physical security is increased, the user experience is improved through a fully digital and seamless process, and data protection requirements are fully complied with and implemented.

Talk to us
+49 6196 9734 090
sales@essentry.com

About essentry
essentry is an enterprise-grade visitor management platform to secure and manage the entire cycle of visitor operations. With a unique visitor verification process that uses both identity card authentication and face matching, essentry leverages artificial intelligence and biometric technology to make customer facilities safer and more secure. This automated process integrates seamlessly into existing IT systems and replaces inefficient reception procedures. The results delivered are a clear return on investment and an elevated visitor experience without compromising security. essentry originates from the demanding German data center industry where high-security facilities are an absolute necessity. Today, we provide essentry as a managed service that can be used across any industry, organization, or geographic location.