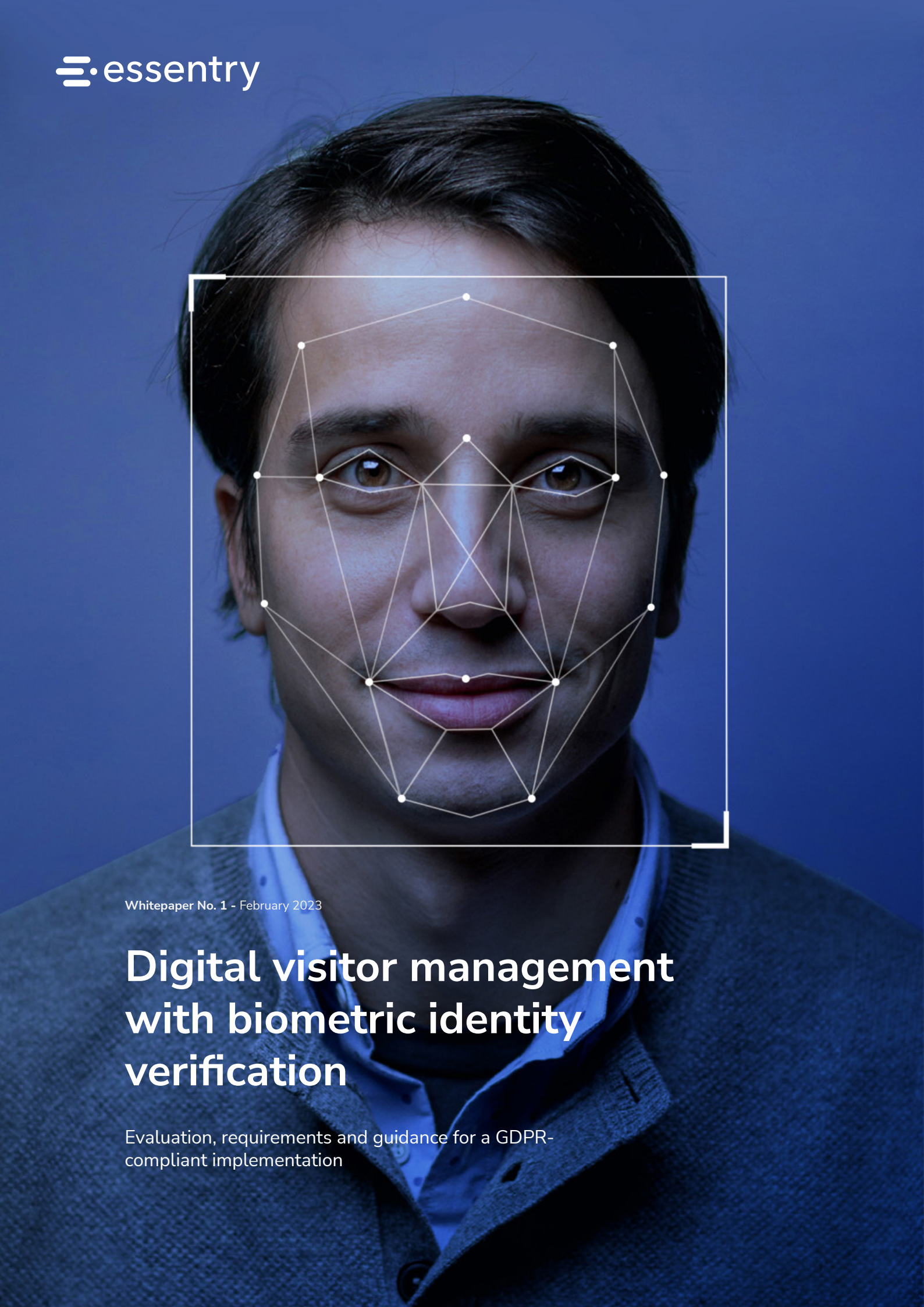
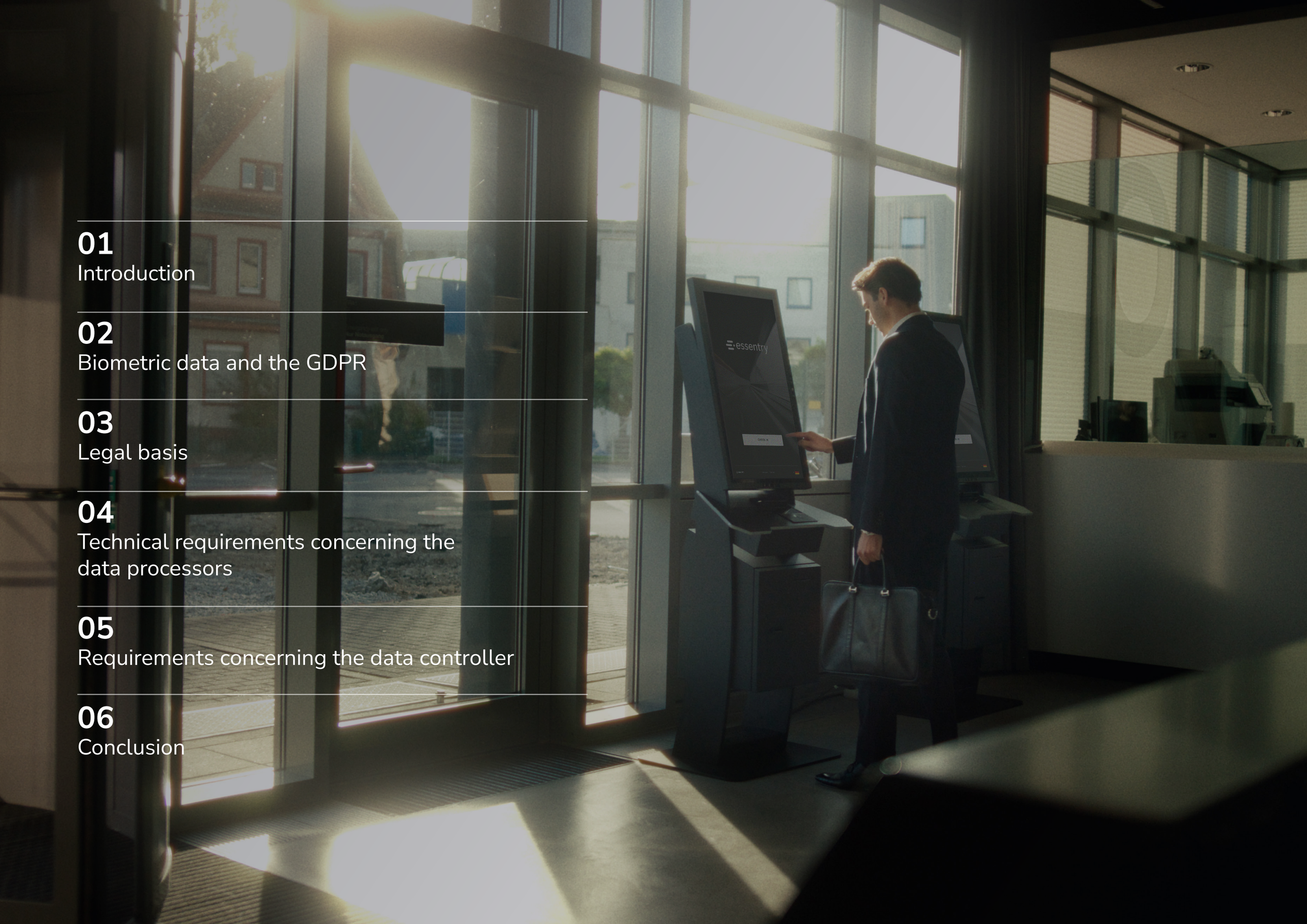
essentry



Whitepaper No. 1 - February 2023

Digital visitor management with biometric identity verification

Evaluation, requirements and guidance for a GDPR-compliant implementation



01
Introduction

In light of increasingly sophisticated security attacks on companies, physical building security is steadily gaining in importance. This is where visitor management plays a decisive role: because an effective visitor management ensures that only authorized individuals are granted access to company buildings.

The so-called “storming of the Capitol” in January 2021 highlighted the far-reaching consequences resulting from uncontrolled building access. In this case, not only does the physical damage to the building have to be repaired, but all computers and rooms of the Capitol must be regarded as compromised. Questions such as “Were listening devices placed in the offices of Congress members?” or “Were USB sticks used to download data from computers or install ‘back doors’ allowing unauthorized remote access in the future?” inevitably arise after such an incident. All of these queries must be resolved in the aftermath, as well as all inventory investigated, replaced or remediated.

Manual visitor management processes, which have to meet high security requirements, are cost-intensive, time-consuming and require tedious registration, authentication and approval measures for everyone involved (visitors, guests, security personnel). Digital visitor management systems provide a solution here. The right system can significantly enhance security, increase process efficiency and improve the user experience at the same time.

Modern visitor management systems enable a highly secure access process for visitors that is largely automated. This is possible through biometric identity verification that integrates into existing access control systems. Automated identity verification involves the use of biometric features, such as a person’s face, which are compared to a reference such as an ID document that has already been checked for authenticity. It is also imperative that the resulting increase in physical security be combined with a sophisticated data security and protection concept, since the data collected is particularly worthy of protection.

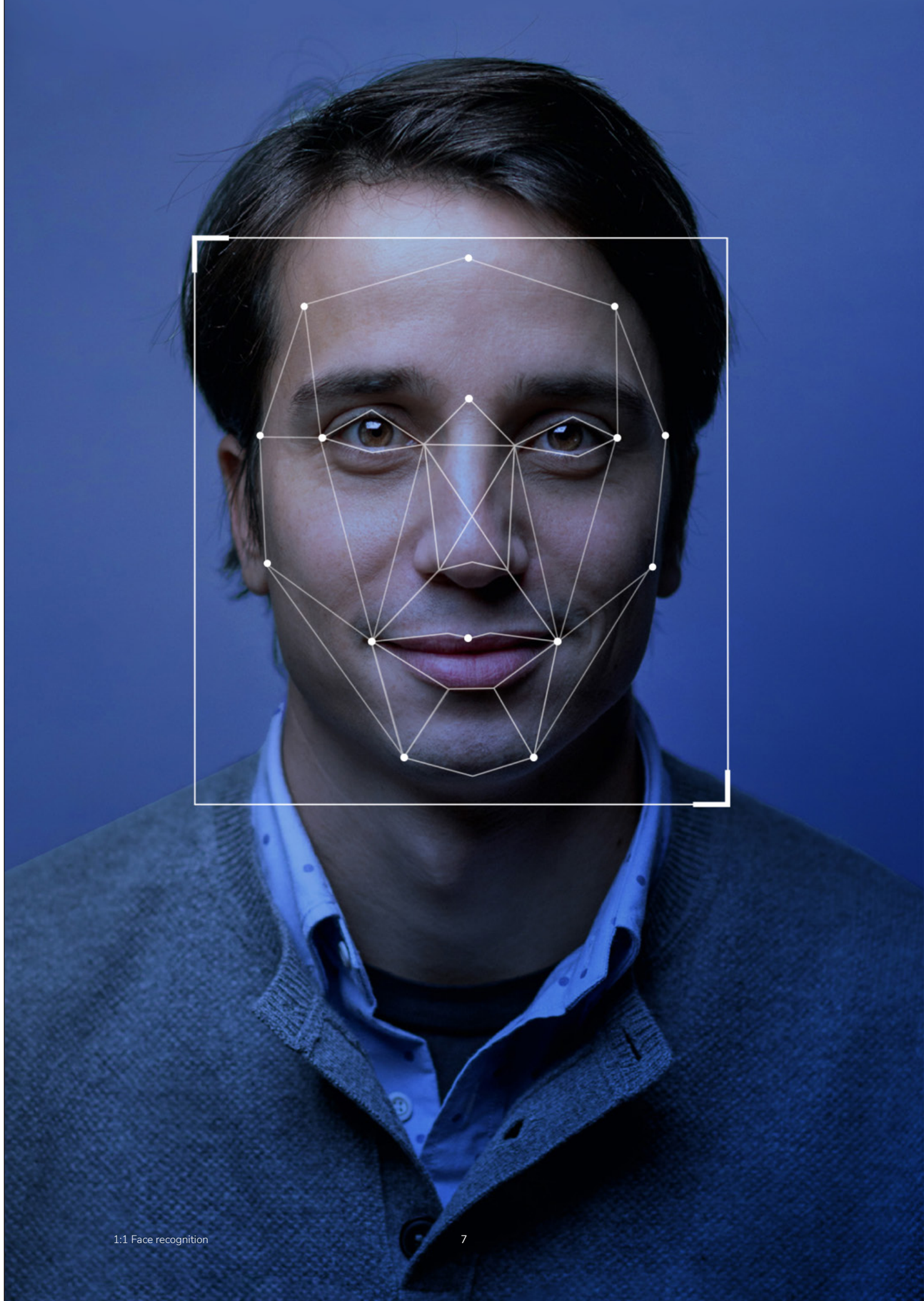
Within the EU, the processing of biometric data is clearly regulated in the General Data Protection Regulation (GDPR). In this white paper, we explain the requirements for a GDPR-compliant use of digital visitor management systems in which biometric data is processed (hereafter referred to as a biometric visitor management system).

02
Biometric data and the GDPR

The processing of biometric data refers to data as defined under Article 9 of the GDPR. This article also stipulates the conditions under which biometric data can be processed. In addition to the GDPR, European and German data protection institutions have both individually and collaboratively concerned themselves with the processing of biometric data, which has been covered in detail through the data protection supervisory bodies of the Federal and State Data Protection Authorities (DSK). In this white paper, we rely on the information contained in the "Guidelines on Facial Recognition"[1] of the European Convention on Data Protection and on the "Position Paper on Biometric Analysis"[2] of the German Data Protection Authority (DSK). The following sections describe the requirements that must be fulfilled, particularly in accordance with the sources listed above, in order to ensure a biometric visitor management system is legally compliant.

1 https://essentry.com/wp-content/uploads/2023/01/T-PD202003rev4-final-Guidelines-Facial-Recognition.docx.pdf

2 https://essentry.com/wp-content/uploads/2023/01/20190405_oh_positionspapier_biometrie.pdf



1:1 Face recognition

03
Legal basis

Biometric data may be processed if an exception is made in accordance with Article 9 (2) of the GDPR. The following is an explanation of the exception (consent) relevant to the context of biometric visitor management systems.

Consent

Obtaining consent from the data subjects (customers, visitors, contractual partners, etc.) forms the primary legal basis under Art. 9 (2) lit. a, Art. 6 (1) lit. a GDPR.
In order for consent to be considered lawful, the requirements of Art. 7 of the GDPR must be met; particularly, the consent must be given voluntarily and the data subject must be informed about the essential points of data processing.
To meet the requirement for voluntary consent, the visitor must be given the choice of whether or not to give consent. The visitor (i.e., the data subject) must not suffer any disadvantages from withholding consent. In practice, this must be ensured by providing an alternative access process, for example through a manned reception desk or a manual identity confirmation by the host when the guests are received in the reception area of the building.

04
Technical requirements concerning the data processor

The technical requirements for the use of biometric visitor management systems include: processing security on the one hand, and data protection-friendly product pre-settings on the other.

Security of Processing

The data processor, i.e., the provider and operator of the visitor management system, must be able to demonstrate that suitable measures are in place that guarantee secure data processing. These should be documented in the order processing contract. Suitable measures include, among others:

- The provider's compliance with the GDPR is continually monitored by an independent, third-party data protection officer.
- All stored data is encrypted according to AES-256.
- All data is encrypted during transmission according to TLS.
- Developers use an encrypted connection (SSH, SSL/TLS) to the systems.
- The databases are hosted in a highly secure data center in Germany.
- The system is regularly subjected to penetration tests performed by independent, specialized companies.
- The provider can provide proof of an information security certification, such as the ISO27001 according to the BSI IT-Grundschutz (basic protection regulation).

Information security certification

It is possible for data processors to receive certification through recognized third-party and governmental institutions such as the German Federal Office for Information Security (BSI). A certificate allows a data processor to prove that a product or service meets defined security requirements. In addition, independent audits conducted by the BSI promote transparency and help build trust in the processor of personal data.

Providers of biometric visitor management systems that can show a certification ISO 27001 on the basis of the BSI IT-Grundschutz basic protection level demonstrate a high level of commitment to transparency and data security. To receive an certificate, a BSI-certified auditor must inspect all reference documents created by the organization, conduct an on-site examination and create an audit report, which is then sent to the BSI for review. The BSI then decides whether to issue a certificate based on the audit results.

Certification is especially relevant for data processors serving the critical infrastructure sectors, since these are essential to maintaining a functional society. The BSI defines these sectors in section 10 (1) of the BSI-Act (Kritis Regulation) as pertaining to energy, information technology and telecommunications, transport, health, water, food, finance and insurance as well as municipal waste disposal. A failure or impairment of the critical infrastructure would cause supply shortages and/or threaten public safety.

Data protection by design and by default

In addition to the aforementioned measures, which mainly concern the infrastructure surrounding the product, the biometric visitor management system should also have data protection-friendly pre-settings that are configured to be especially sensitive in regard to personal data, also referred to as “privacy by design or default” according to Art. 25 (2) GDPR. Particularly 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:

- A verification of ID documents must always take place on a local end device, so that the entire ID document is never processed in the cloud.

- No images of the ID document should be stored locally either, but instead deleted immediately after verification.

- There should only be biometric verification, not 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 corresponding feature displayed on the user ID. This is equivalent to a data-saving 1:1 comparison.

- In contrast: With biometric identification, the biometric feature is compared to all of the reference features stored in the system.

- This is equivalent to a 1:n comparison, in which an arbitrarily large amount of data must be processed.

In practice, it is often the case that the use of modern digital visitor management systems not only enables the above-mentioned requirements to be met, but actually increases data protection compared to manual visitor management. The following table compares the typical manual process with a data protection-friendly digital process.

ID-
Verification

3D-real time
portrait

Biometric face
matching

Typical manual process

Insufficient verification

Typically, humans are not able to verify IDs from all different countries and check whether the ID contains all the important security features. Additionally, it can be unpleasant to have to hand over one's identity card to a stranger for verification.

Manual face match

The human eye performing face matches has proven to be significantly more error-prone than face matches conducted by computer-based algorithms.

Manual data processing and non-transparent retention policies

Typically, visitor data is stored and shared in multiple systems or paper logbooks, to which multiple people have access. Retention and deletion policies of these systems are often not enforced.

Non-transparent data protection policies and user consent forms

If at all, privacy policies are typically only presented in paper form, consent forms are not stored centrally or are not traceable (e.g., for audits).

Data protection-friendly digital process

Local verification of the identity document (ID) at the kiosk

Verification of the ID document by taking photos at the kiosk with three different light sources to check if the document has all security features. The images are immediately deleted after the verification.

1:1 face match

Achieved by matching a person's photo ID with a selfie photo taken of the person in front of the kiosk only.

Allows custom viewing settings and data retention periods

The system can be configured to meet customer needs and offers various options on the landing page (e.g., show selfie or not). Custom retention periods / deletion rules can be individually configured for each data category.

Privacy and user consent

References to the privacy policy are made available at multiple points during the process, e.g. via:

- Link to the privacy policy in an invitation, online check-in or on the kiosk screen.
- Notice in the invitation email that an identification document is required for on-site registration due to high-security requirements.
- Customizable to require additional explicit consent at online check-in or on-site at the kiosk screen.

05
Requirements concerning the data controller

The data controller (i.e., the customer responsible for the use of the digital visitor management system) should ensure the following measures have been implemented before introducing a biometric visitor management system. The leading providers of biometric visitor management systems help their customers achieve these measures via document templates and informational resources.

Data Impact Assessment Test

Whenever innovative technologies are used, Article 35 (1) GDPR requires that a data protection impact assessment be conducted. This obligation is also included in the so-called "must list" of the supervisory authorities, according to Article 35 (4) GDPR, according to which the controller must always conduct an impact assessment when using biometric access systems. This must list foreseeable risks to the rights and freedoms of data subjects and assess the impact of the intended processing operations.

The data protection impact assessment for the use of biometric visitor management systems should list fundamental technical risks and their corresponding protective measures.

In addition, each individual risk should be assessed based on its the probability of occurrence. Furthermore, customer-specific risks can be determined with those responsible in order to include individual organizational risks in the impact assessment. 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 now used by almost every smartphone user.

Data Processing Agreement

To cover more of the legal framework on the use of biometric visitor management systems: It is essential that appropriate contracts for processing be made in accordance with Art. 28 of the GDPR. These contracts transparently regulate the rights and obligations for both the client and the contractor (the data controller and data processor). The system provider should be able to present a contract for this purpose.

Information obligations and data subject rights

Data controllers must comply with their obligations to provide information about the data collected pursuant to Art. 12-14 GDPR in an easily accessible form. All rights of the data subjects as well as of the recipients of the personal data must be presented transparently in a privacy statement. The information obligations should be made available during the registration and check-in process.

Modern visitor management systems offer customers the option of storing their own data privacy statements in the registration interface and also provide support in the form of text templates. It is also advisable to introduce a process for responding effectively and on time to data subjects' rights, such as requests for information under Art. 15 of the GDPR. Leading visitor management software providers have implemented processes to help the responsible entities respond simply and quickly to data subject requests, so that the legal deadline of 14 days can always be met.

06
Conclusion

In summary, it is possible to introduce a biometric visitor management system fully in compliance with the law, so long as the prerequisites described in this white paper and any company-specific requirements are followed. The GDPR provides clear regulations in this respect, and statements from data protection authorities provide further clues for implementation. The leading providers of visitor management systems guide their customers through this process step-by-step and work closely with the respective legal departments or data protection officers to ensure that all requirements are met. This can solve what at first glance appears to be a paradox: the physical security is enhanced, the user experience is transformed into a fully digital and seamless process and yet, data protection requirements are implemented and fully compliant.

About essentry

essentry specializes in the digitalization of access processes. The core product is the verification of personal identities at border-control level and the automation of the access process. Using biometric technology and artificial intelligence, essentry is able to achieve the highest level of security for facilities, employees and guests. essentry integrates seamlessly into existing systems and IT landscapes and increases security to the highest possible level. Because it originated in the demanding data center industry, essentry is characterized by the stringent security requirements prevailing there and adheres to strict regulations regarding data protection, data security and compliance. In addition, essentry has integrated these standards into its products and offers them as a managed service, so that other organizations and industries may easily apply them.

Essentry GmbH | Düsseldorfer Straße 15 | 65760 Eschborn | +49 (0) 6196 9734 090 | info@essentry.com