essentry

Whitepaper No. 1 - Februar 2023

Digitales Besuchermanagement mit biometrischer Identitätsverifikation

Bewertung, Voraussetzungen und Leitfaden für eine DSGVO-konforme Einführung

01
Einführung

Die physische Gebäudesicherheit gewinnt in Zeiten von immer raffinierteren Sicherheitsangriffen auf Unternehmen stetig an Bedeutung. Dabei spielt der Besuchermanagementprozess eine entscheidende Rolle. Denn durch ein effektives Besuchermanagement wird sichergestellt, dass nur autorisierte Personen Zutritt zu den Unternehmensgebäuden erhalten.

Es brauchte nur eine überzeugende Täuschung, um ein gesamtes Firmennetzwerk zu kompromittieren. In einem dokumentierten Fall in einem Bürogebäude in Brüssel verschaffte sich eine Person mit dem Vorwand, ein Techniker eines bekannten Internetanbieters zu sein, Zutritt zum Gebäude – ohne verlässliche Identitätsprüfung. Der Eindringling gelangte in den Serverraum und installierte manipulierte Hardware, die das Netzwerk potenziell vollständig kompromittierte. Der Vorfall blieb unentdeckt und fiel erst durch auffällige Datenverkehrsmuster auf. Dieser Fall zeigt eindrücklich, wie leicht physische Sicherheitslücken und fehlende Kontrollmechanismen ausgenutzt werden können, um Zugang zu kritischer Infrastruktur zu erlangen. Die Folgen waren ein umfassendes Sicherheitsaudit, der Austausch von Hardware und die Benachrichtigung betroffener Kunden – mit erheblichen betrieblichen und reputativen Auswirkungen.

Dabei sind manuelle Besuchermanagementprozesse, die hohe Sicherheitsanforderungen erfüllen müssen, kostenintensiv und gehen für alle involvierten Personen (Besucher, Gastgeber, Sicherheitspersonal) mit zeitaufwändigen, mühsamen Anmelde-, Authentifizierungs- und Genehmigungsschritten einher. Digitale Besuchermanagementsysteme schaffen hier Abhilfe.

Mit dem richtigen System kann gleichzeitig die Sicherheit deutlich erhöht, die Prozesseffizienz gesteigert und die Nutzererfahrung verbessert werden. Moderne Besuchermanagement-systeme ermöglichen einen weitestgehend automatisierten hochsicheren Zutrittsprozess für Besucher. Dies wird durch eine biometrische Identitätsverifikation in Verbindung mit einer Integration in bestehende Zutrittskontrollsysteme ermöglicht. Bei der automatisierten Identitätsverifikation werden biometrische Merkmale, wie das Gesicht, mit einer Referenz, wie beispielsweise ein auf Echtheit geprüftes Ausweisdokument, abgeglichen. Die dadurch erhöhte physische Sicherheit muss mit einem ausgereiften Datensicherheits- und Datenschutzkonzept kombiniert werden, denn die erhobenen Daten sind besonders schützenswert.

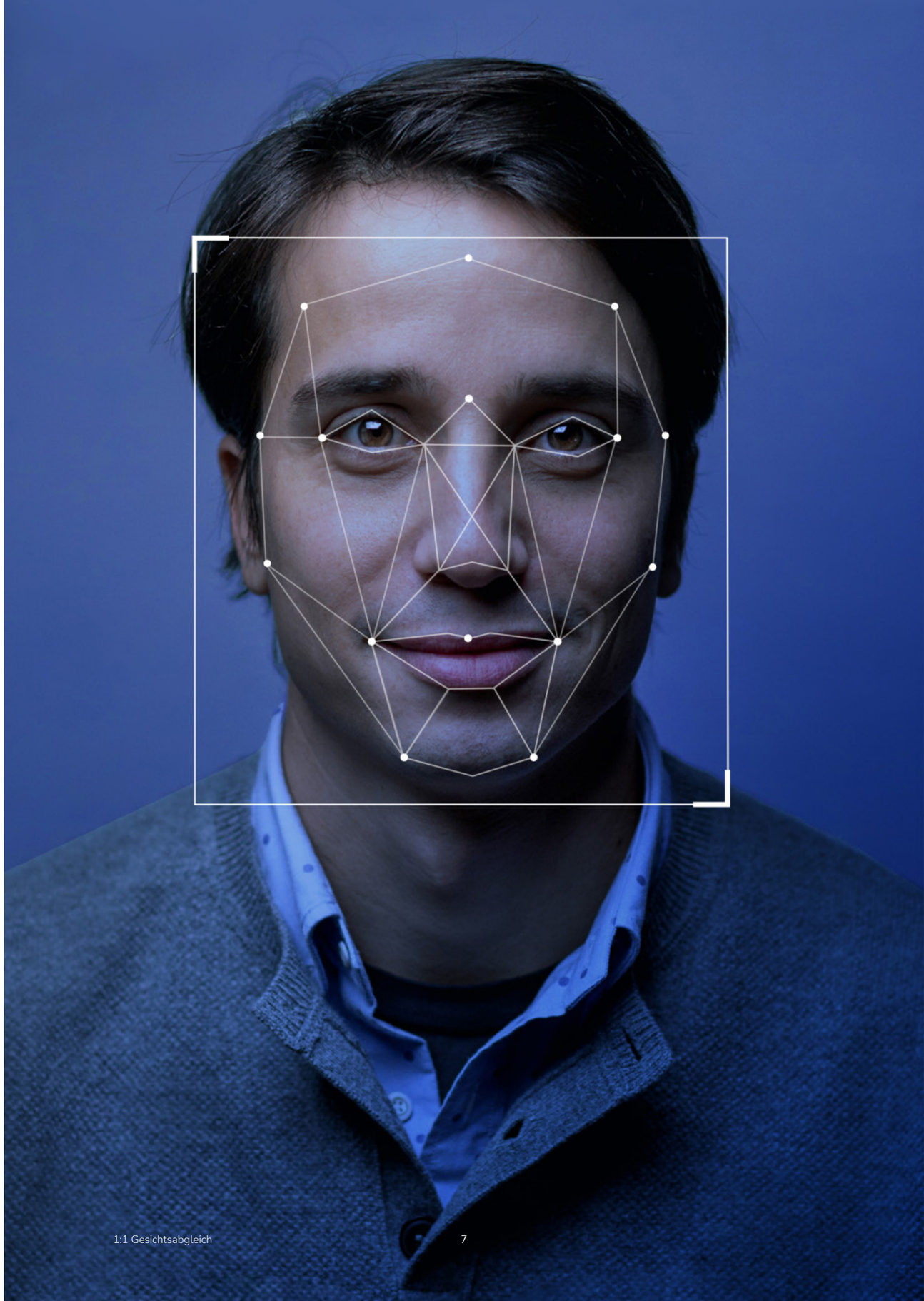
Innerhalb der EU ist die Verarbeitung biometrischer Daten in der Datenschutz-Grundverordnung (DSGVO) klar geregelt. In diesem Whitepaper erläutern wir die Anforderungen an einen DSGVO konformen Einsatz von digitalen Besuchermanagementsystemen, bei denen biometrische Daten verarbeitet werden (nachfolgend auch biometrisches Besucher-managementsystem).

02
Biometrische Daten und die DSGVO

Bei der Verarbeitung von biometrischen Daten handelt es sich um Daten gemäß Artikel 9 DSGVO. In diesem Artikel wird auch geregelt, unter welchen Voraussetzungen biometrische Daten verarbeitet werden können. Neben der DSGVO, haben sich europäische und deutsche Datenschutzorgane individuell sowie gemeinsam über Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) im Detail mit der Verarbeitung biometrischer Daten auseinandergesetzt. In diesem Whitepaper stützen wir uns unter anderem auf die Informationen in den „Guidelines on Facial Recognition“[1] der europäischen Datenschutzkonvention, sowie auf das "Positionspapier zur biometrischen Analyse"[2] der DSK. Die folgenden Abschnitte geben die Voraussetzungen wieder, die auf Grundlage insbesondere der vorgenannten Quellen erfüllt sein müssen, um eine rechtskonforme Einführung eines biometrischen Besuchermanagementsystems zu gewährleisten.

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 Gesichtsabgleich

03
Rechtsgrundlage

Biometrische Daten dürfen bei Vorliegen eines gem. der in Art. 9 Abs. 2 DSGVO normierten Ausnahmetatbestandes verarbeitet werden. Dieser Artikel listet die möglichen Ausnahmetatbestände auf. Nachfolgend wird der für den Kontext von biometrischen Besuchermanagementsystemen relevante Ausnahmetatbestand (Einwilligung) erläutert.

Einwilligung

Die Einholung einer Einwilligung der Betroffenen (Kunden, Besucher, Vertragspartner etc.) gem. Art. 9, Abs. 2 lit. a, Art. 6 Abs. 1 lit. a DSGVO dient als Rechtsgrundlage für die Verarbeitung der biometrischen Daten. Damit die Einwilligung rechtlich wirksam ist, müssen die Voraussetzungen des Art. 7 DSGVO erfüllt werden. Die Einwilligung muss insbesondere freiwillig erfolgen und der/die Betroffene muss über die wesentlichen Punkte der Datenverarbeitung informiert werden. Um die Anforderung der Freiwilligkeit der Einwilligung zu erfüllen, muss dem Besucher die Wahl überlassen werden, ob er die Einwilligung abgibt oder nicht. Für den Fall der Nichtabgabe der Einwilligung dürfen dem Besucher (also dem Betroffenen) keine Nachteile entstehen. Dies ist in der Praxis dadurch sicherzustellen, dass ein alternativer Zutrittsprozess zur Verfügung gestellt wird, beispielsweise durch einen besetzten Empfang oder einer manuellen Identitätsbestätigung durch den Gastgeber bei Abholung der Gäste im Empfangsbereich des Gebäudes.

04
Technische Voraussetzungen seitens des Auftragsverarbeiters

Die technischen Voraussetzungen für den Einsatz biometrischer Besuchermanagementsysteme umfassen zum einen die Sicherheit der Verarbeitung und zum anderen datenschutzfreundliche Voreinstellungen, die produktseitig konfiguriert werden können.

Sicherheit der Verarbeitung

Der Auftragsverarbeiter, also der Anbieter und Betreiber des Besuchermanagement-systems muss geeignete Maßnahmen nachweisen können, die eine sichere Datenverarbeitung gewährleisten. Diese sollten im Auftragsverarbeitungsvertrags dokumentiert sein. Geeignete Maßnahmen umfassen unter anderem:

- Die Einhaltung der DSGVO durch den Anbieter wird von einem unabhängigen, externen Datenschutzschutzbeauftragten kontinuierlich überwacht.

- Alle gespeicherten Daten werden gemäß AES-256 verschlüsselt.

- Alle Daten werden während der Übertragung gemäß TLS verschlüsselt.

- Entwickler nutzen eine verschlüsselte Verbindung (SSH, SSL/TLS) zu den Systemen.

- Die Datenbanken werden in einem hochsicheren Rechenzentrum in Deutschland gehosted.

- Das System wird regelmäßig Penetrations-Tests unterzogen, die durch unabhängige, spezialisierte Unternehmen durchgeführt werden.

- Der Anbieter kann eine Informationssicherheits-Zertifizierung nachweisen, wie z.B. die ISO 27001 nach BSI IT-Grundschutz.

BSI-Zertifizierung der Informationssicherheit

Datenverarbeiter können sich durch anerkannte dritte und staatliche Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizieren lassen. So lässt sich nachweisen, dass ein Produkt oder eine Dienstleistung definierte Sicherheitsanforderungen erfüllt. Darüber hinaus fördern unabhängige Audits des BSI die Transparenz und tragen dazu bei, Vertrauen in den Verarbeiter personenbezogener Daten aufzubauen.

Anbieter von biometrischen Besuchermanagementsystemen, die eine ISO 27001 Zertifizierung auf Basis des BSI IT-Grundschutzes vorweisen können, zeigen ein hohes Maß an Transparenz und Datensicherheit. Um ein solches Zertifikat zu erhalten, muss ein BSI-zertifizierter Auditor alle von der Organisation erstellten Referenzdokumente einsehen, eine Vor-Ort-Prüfung durchführen und einen Auditbericht erstellen, der zur Freigabe an das BSI geschickt wird. Das BSI entscheidet dann auf der Grundlage der Auditergebnisse über die Erteilung eines Zertifikats.

Die Zertifizierung ist insbesondere für Datenverarbeiter in den Bereichen der kritischen Infrastrukturen relevant, da diese für die Aufrechterhaltung einer funktionierenden Gesellschaft unerlässlich sind. Das BSI definiert diese Sektoren in § 10 Abs. 1 BSI-Gesetz (KRITIS-Verordnung) als die Bereiche Energie, Informationstechnik & Telekommunikation, Verkehr & Transport, Gesundheit, Wasser, Ernährung, Finanz- & Versicherungswesen, Staat & Verwaltung, Medien & Kultur sowie Siedlungs-Abfallentsorgung. Ein Ausfall oder eine Beeinträchtigung der kritischen Infrastrukturen würde zu Versorgungsengpässen führen und/oder die öffentliche Sicherheit gefährden.

Datenschutzfreundliche Voreinstellungen

Neben den vorgenannten Maßnahmen, die vor allem die Infrastruktur des Produktes betreffen, sollte das biometrische Besuchermanagementsystem datenschutzfreundliche Voreinstellungen mitbringen. Insbesondere bei der Verarbeitung von Daten aus Ausweisdokumenten muss genau dokumentiert sein, welche Daten tatsächlich verarbeitet und gespeichert werden. Nachfolgend sind die wichtigsten Aspekte aufgeführt:

- Eine Ausweisverifikation sollte immer lokal auf einem Endgerät stattfinden, sodass niemals das gesamte Ausweisdokument cloud-seitig verarbeitet wird.

- Auch lokal sollte kein Bild des Ausweisdokuments gespeichert werden, sondern nach der Verifikation direkt gelöscht werden.

- Es sollte nur eine biometrische Verifikation stattfinden, keine biometrische Identifikation.

- Bei der biometrischen Verifikation gibt der Nutzer dem System seine Identität vorab bekannt (z. B. durch das Scannen eines ihm zugeordneten QR-Codes), das System vergleicht das biometrische Merkmal (das Gesicht) dann nur mit dem einen zur User-ID passenden Referenzmerkmal. Dies entspricht einem datensparsamen 1:1-Vergleich.

- Im Gegensatz dazu wird bei der biometrischen Identifikation das biometrische Merkmal mit allen im System gespeicherten Referenzmerkmalen verglichen. Dies entspricht einem 1:n-Vergleich, bei dem eine beliebig große Datenmenge verarbeitet wird.

- Löschfristen sollten durch den Kunden (d.h. die verantwortliche Stelle) für die verschiedene Datenarten konfiguriert werden können.

- Das System sollte die Möglichkeit bieten, dem Nutzer Datenschutzerklärungen anzuzeigen und ggf. Einwilligungen der Nutzer für eine Datenverarbeitung einzuholen und personenbezogen zu speichern.

In der Praxis ist es häufig so, dass durch den Einsatz moderner digitaler Besucher managementsysteme nicht nur die vorgenannten Anforderungen erfüllt werden können, sondern der Datenschutz im Vergleich zu manuellen Besucher-managementprozessen sogar erhöht wird. In der nachfolgenden Tabelle wird der typische manuelle Prozess einem datenschutzfreundlichen digitalen Prozess gegenübergestellt.

Ausweis-verifikation

3D-Echtzeit-Porträt

Biometrischer Gesichtsabgleich

Üblicher manueller Prozess

Unvollständige Validierung

Das menschliche Auge ist nicht in der Lage, die Echtheit von Ausweis-Dokumenten zu überprüfen. Zusätzlich gibt der Besucher seinen Ausweis bei der Sichtüberprüfung aus der Hand.

Manuelle Gesichtserkennung

Fehleranfälliger manueller Gesichtsabgleich durch Empfangspersonal.

Manuelle Datenverarbeitung und intransparente Aufbewahrungsfristen

Typischerweise werden Besucherdaten in mehreren Systemen oder Formularen gespeichert und gemeinsam genutzt. Aufbewahrungs- und Löschrichtlinien werden oft nicht durchgesetzt.

Intransparente Datenschutzrichtlinien und Zustimmung der Benutzer

Wenn überhaupt, werden Datenschutzrichtlinien typischerweise nur in Papierform dargestellt und Einwilligungen werden nicht zentral gespeichert oder sind nicht nachvollziehbar (z. B. für Audits).

Datenschutzfreundlicher digitaler Prozess

Validierung des Ausweis-Dokuments vor Ort am Gerät

Überprüfung des Ausweises auf relevante Sicherheitsmerkmale, mit drei verschiedenen Lichtquellen. Die Fotos des Dokuments werden sofort nach der Validierung gelöscht.

1:1 Gesichtsabgleich

Erfolgt durch den Abgleich des ausgeschnittenen Fotos aus dem Ausweis-Dokument mit dem 3D-Tiefenkamera aufgenommenen Echtzeitportrait.

Benutzerdefinierte Ansicht und Datenaufbewahrungszeiträume zulassen

Das System ist nach den Bedürfnissen des Kunden konfigurierbar und bietet in der Empfangsansicht verschiedene Optionen (z.B. Echtzeitportrait anzeigen oder nicht). Für jede Datenkategorie können benutzerdefinierte Aufbewahrungsfristen / Löschregeln individuell konfiguriert werden.

Datenschutz und Benutzereinwilligung

Verweis (anpassbar) auf die Datenschutzrichtlinie an mehreren Stellen im Prozess, z. B.

- Link zur Datenschutzerklärung in der Einladung, beim Online-Check-in und auf dem Kioskbildschirm.
- In der Einladungs-E-Mail wird darauf hin gewiesen, dass für die Registrierung vor Ort aufgrund von Hochsicherheitsanforder-ungen ein Ausweisdokument erforderlich ist.
- Anpassbar, um vor Ort auf dem Kiosk-Bildschirm zusätzlich eine ausdrückliche Einwilligung einzuholen.

05
Voraussetzungen für die verantwortliche Stelle

Auf Seiten der verantwortlichen Stelle, sollten vor Einführung des biometrischen Besuchermanagementsystems die nachfolgenden Maßnahmen durchgeführt werden. Führende Anbieter von biometrischen Besuchermanagementsystemen unterstützen den Kunden bei der Durchführung der Maßnahmen mit Dokumentenvorlagen und Informationen.

Datenschutzfolgenabschätzung

Werden innovative Technologien eingesetzt, ist nach Art. 35 Abs. 1 S. 1 DSGVO die Durchführung einer Datenschutzfolgenabschätzung notwendig. Diese Pflicht findet sich ebenfalls in der sogenannten “Muss-Liste” der Aufsichtsbehörden, nach Art. 35 Abs. 4 S. 1 DSGVO, wonach bei Einsatz biometrischer Zutrittssysteme die verantwortliche Stelle in jedem Fall eine Folgenabschätzung durchführen muss. In dieser müssen voraussichtliche Risiken für die Rechte und Freiheiten betroffener Personen aufgeführt und die Folgen der vorgesehenen Verarbeitungsvorgänge abgeschätzt werden. Die Datenschutzfolgenabschätzung für den Einsatz von biometrischen Besuchermanagementsystemen sollte grundsätzliche technische Risiken und jeweils entsprechende Schutzmaßnahmen aufführen.

Zusätzlich sollte die Eintrittswahrscheinlichkeit jedes einzelnen Risikos bewertet werden. Weiterhin können kundenspezifische Risiken mit den jeweiligen Verantwortlichen ermittelt werden, um auch individuelle organisatorische Risiken in die Folgenabschätzung mit einzubeziehen.

In der Datenschutzfolgenabschätzung ist zu berücksichtigen, dass - trotz der hohen gesetzlichen Vorgaben - der Einsatz von biometrischen Zutritts- und Zugangskontrollen ein Massenphänomen geworden ist. So werden Technologien wie beispielsweise Fingerabdrucksensor oder „Face Unlock“ heute von nahezu jedem Smartphone Nutzer genutzt.

Auftragsverarbeitungsvertrag

Um weitere rechtliche Rahmenbedingungen für den Einsatz biometrischer Besuchermanagementsysteme abzudecken, sind entsprechende Verträge zur Auftragsverarbeitung nach Art. 28 DSGVO abzuschließen. Diese Verträge regeln transparent die Rechte und Pflichten sowohl für Auftraggeber als auch Auftragnehmer. Hierfür sollte der Anbieter des Systems einen Vertrag vorlegen können.

Informationspflichten und Betroffenenrechte

Verantwortliche Stellen müssen in leicht zugänglicher Form ihren Informationspflichten nach Art. 12-14 DSGVO nachkommen. Sämtliche Rechte der betroffenen Personen sowie die Empfänger der personenbezogenen Daten werden in einer Datenschutzerklärung transparent dargestellt.

Die Informationspflichten sollten im Zuge des Registrierungs- und Check-in Prozesses zur Verfügung gestellt werden. Moderne Besuchermanagementsysteme bieten dem Kunden in der Administrationsoberfläche die Möglichkeit, eigene Datenschutzerklärungen im System zu hinterlegen und unterstützen ebenfalls mit Textvorlagen.
Es empfiehlt sich zudem die Einführung eines Prozesses um Betroffenenrechte wie beispielsweise Auskunftsersuchen nach Art. 15 DSGVO effektiv und fristgerecht zu beantworten. Hier haben führende Besuchermanagement Software Anbieter Prozesse implementiert, um verantwortliche Stellen einfach und zügig bei der Beantwortung von Betroffenenanfragen zu unterstützen, sodass in jedem Fall die gesetzliche Frist von 14 Tagen eingehalten werden kann.

06
Schlussfolgerung

Im Ergebnis ist die Einführung eines biometrischen Besuchermanagementsystems bei Befolgung der in diesem Whitepaper beschriebenen Voraussetzungen und eventuellen unternehmensspezifischer Anforderungen rechtskonform möglich. Hierzu gibt es zum einen in der DSGVO klare Regelungen und die Stellungnahmen der Datenschutzbehörden bieten weitere Umsetzungshinweise. Führende Besuchermanagementsystem Anbieter unterstützen Ihre Kunden bei jedem Schritt und arbeiten eng mit den jeweiligen Rechtsabteilungen bzw. Datenschutzbeauftragten zusammen, um alle Voraussetzungen zu erfüllen. So kann gelöst werden, was auf den ersten Blick wie ein Dilemma erscheint: Die physische Sicherheit wird erhöht, die Nutzererfahrung durch einen vollständig digitalen und reibungslosen Prozess verbessert und die Vorgaben des Datenschutzes werden vollständig eingehalten und umgesetzt.

Über essentry

essentry ist auf die Digitalisierung von Zutrittsprozessen spezialisiert. Kern des Produktes ist die Verifikation von Identitäten auf Grenzkontrollniveau und das Automatisieren von Zutrittsprozessen. Durch den Einsatz biometrischer Technologie und künstlicher Intelligenz realisiert essentry ein Höchstmaß an Sicherheit für Einrichtungen, Mitarbeiter und Gäste. essentry integriert sich nahtlos in bestehende Prozesse und IT-Landschaften und erhöht die Sicherheit auf ein Höchstmaß. Seinen Ursprung hat essentry in der anspruchsvollen Rechenzentrumsindustrie und ist geprägt von den dort herrschenden Hochsicherheitsanforderungen sowie den strengen Regularien an Datenschutz, Datensicherheit- und Compliance-Standards. Um auch anderen Organisationen und Industrien die Anwendung zu ermöglichen, hat essentry die Standards in seinen Produkten industrialisiert und bietet sie als Managed-Service an.

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