TILLTRÄDESKONTROLL VIA **ANSIKTSIGENKÄNNING.**

EN **GUIDE** FRAMTAGEN AV BOON EDAM

BOON EDAM
YOUR **ENTRY** EXPERTS.

INTRODUKTION.

I denna guide förklaras hur tillträdeskontroll via ansiktsigenkänning fungerar. Här nämns också vilka faktorer du bör överväga när du väljer ett tillträdeskontrollsystem med ansiktsigenkänning. Ansiktsigenkänningsteknik är något relativt nytt på marknaden, därför undrar du kanske vilka aspekter som kan spela en viktig roll i tillämpningen av denna teknik. Denna guide ger dig bättre insikt i vad tillträdeskontroll via ansiktsigenkänning egentligen innebär och vad du bör överväga när du köper ett sådant system.

TYPER AV **BIOMETRISK INFORMATION**

Biometriska kännetecken är mätbara fysiologiska egenskaper som kan användas för att beskriva olika människor. Användning av biometrisk information inom tillträdeskontroll-tillämpningar har blivit alltmer populärt. De fyra vanligaste formerna är följande:

IRISAVLÄSNING

Iris eller regnbågshinnan hos varje människa är unik. En irisavläsare identifierar gropar, streck och strimmor i iris och omvandlar dessa till en iriskod. Iriskoden jämförs sedan med användarinformation i en databas varefter tillträde antingen godkänns eller nekas.

AVLÄSNING AV HANDFLATAN

Denna metod innebär att handflatans unika mönster av vener och kapillärer görs mer framträdande med hjälp av NIR-illuminering (near infrared). Vissa handflateavläsare registrerar även kännetecknande drag såsom veck och små knutor på handflatan. Denna information används sedan för att skapa en unik profil som kopplas till en behörig person.

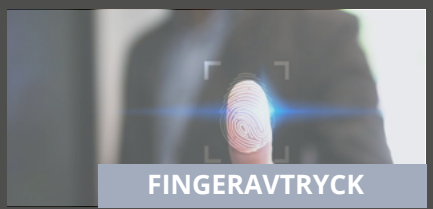
FINGERAVTRYCK

Det finns olika typer av fingeravtryckläsare på marknaden. Dessa enheter avläser det unika mönstret av fina linjer på fingrarnas hud. Beroende på avläsningsresultatet, godkänns eller nekas tillträde.

ANSIKTSIGENKÄNNING

Den sista typen av biometrisk tillträdeskontroll använder sig av ansiktsigenkänning. En bild av ett ansikte tagen med video- eller fotokamera filtreras med hjälp av en algoritm. På bara några millisekunder registreras ansiktets kännetecknande drag och omvandlas till en unik kod.

Ansiktsigenkänningsprogramvaran jämför sedan denna kod med användarinformation i en databas. Om koden och informationen matchar, identifieras individen på bilden varefter tillträde godkänns eller nekas.



ANSIKTSIGENKÄNNING

Ansiktsigenkänning kan vara praktisk inom många olika tillämpningsområden. I denna guide ligger fokus på tillträdes-kontroll. Olika skillnader inom tillämpningsområdena presenteras kortfattat nedan.

MASSÖVERVAKNING

Vid massövervakning används ansiktsigenkänning för att urskilja en individ i en folkmassa. För att göra detta på ett effektivt sätt krävs specialiserad och effektiv maskinvara och programvara.

PERSONLIG AUTENTISERING

Denna typ av ansiktsigenkänning används ofta i mobila enheter som smarttelefoner och kräver relativt enkel programvara och maskinvara. Denna metod använder ansiktet som ett alternativ till ett lösenord.

BROTTSPLATSUNDERSÖKNING

Ansiktsigenkänning kan även användas för att rekonstruera en individs färdväg baserat på videobilder. Till exempel kan sådan information göra det lättare att identifiera var en rymling befunnit sig under det senaste dygnet.

TILLTRÄDESKONTROLL

Slutligen kan ansiktsigenkänning användas för tillträdeskontroll. Programvaran ska kunna jämföra information från flera kameror med information i databasen i realtid. Baserat på databasens storlek, installeras en server som snabbt verifierar auktorisering så att tillträdespunkten kan öppnas.

I DENNA **GUIDE:**

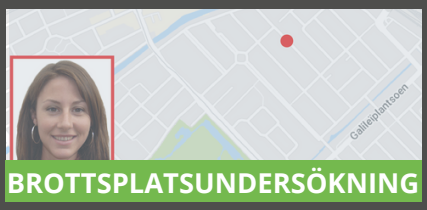
FÖRDELAR MED ANSIKTSIGENKÄNNING

KOMPONENTER I ANSIKTSIGEN-KÄNNINGSTEKNIK

TEKNISKA ASPEKTER

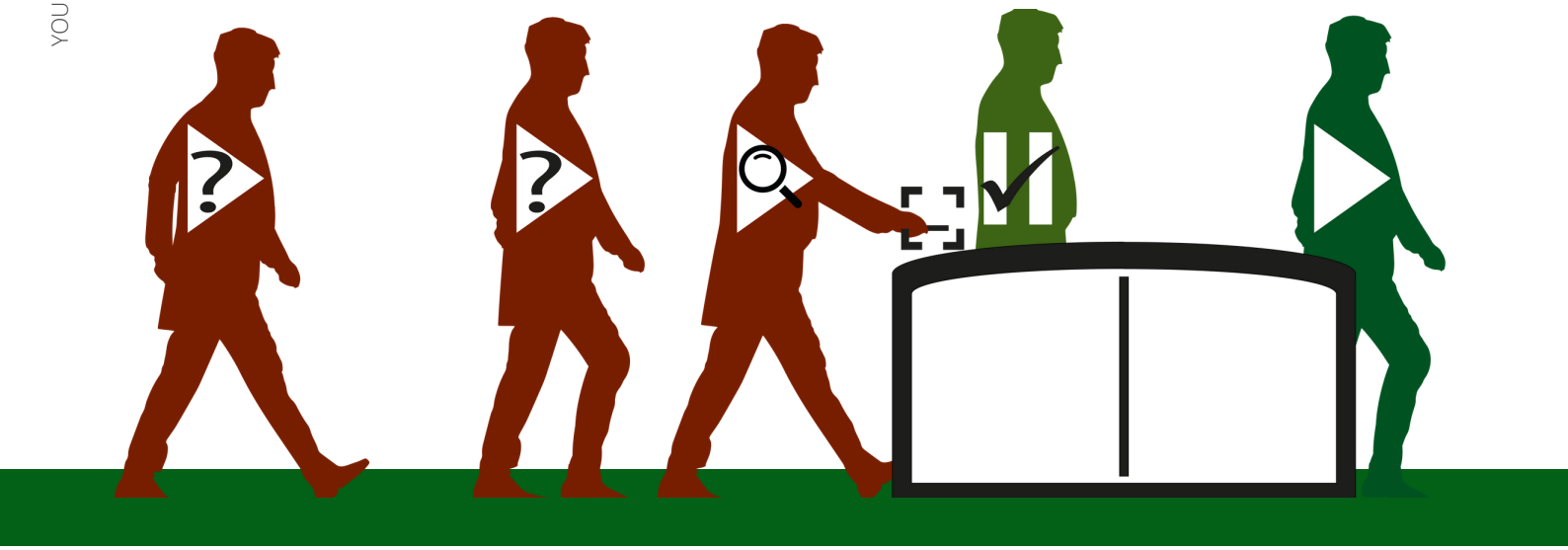
I PRAKTIKEN

DIGITAL SÄKERHET

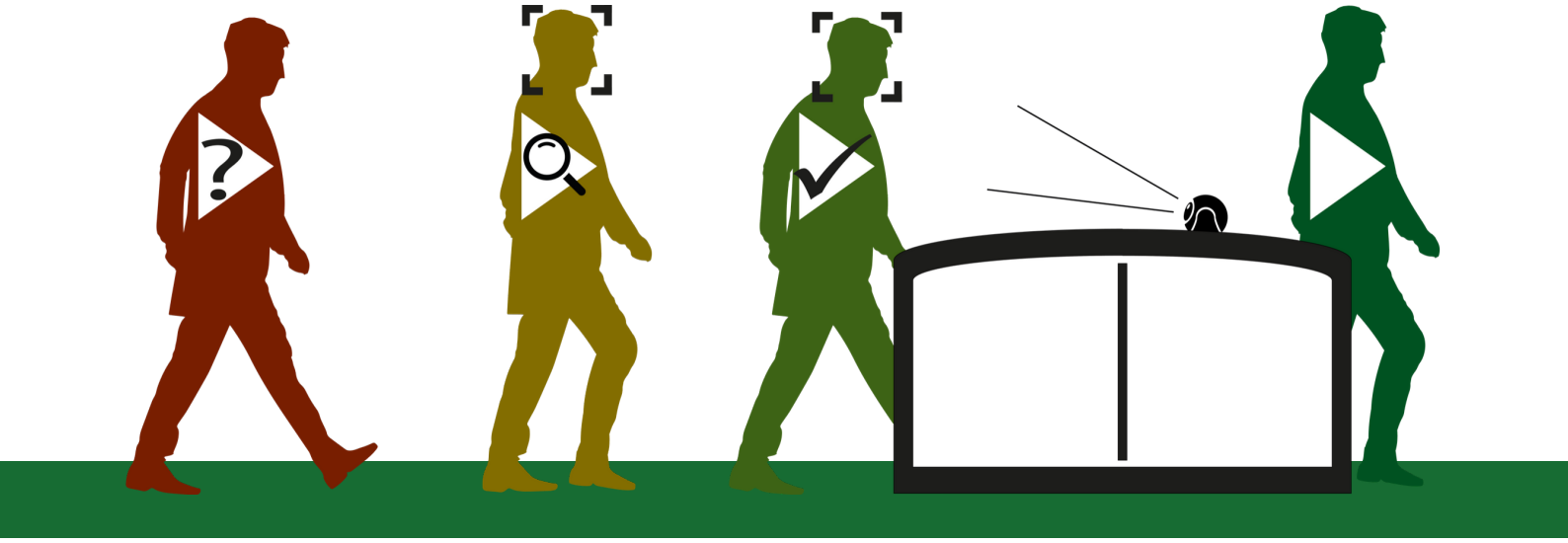


FÖRDELAR
MED ANSIKTSIGENKÄNNING.

TRADITIONELL **KORTLÄSARE**

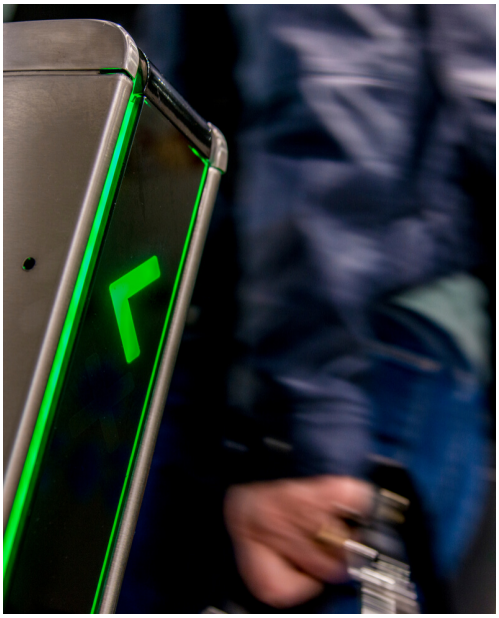


ANSIKTSIGENKÄNNING



FÖRBÄTTRAT **FLÖDE**

En av huvudfördelarna med tillträdeskontroll via ansiktsigenkänning är den minskade väntetiden vid tillträdespunkten. Programvaran registrerar en persons ansikte när denne närmar sig tillträdespunkten och avgör innan personen har kommit ändra fram om tillträde ska godkännas eller ej. När personen befinner sig i närheten av eller vid tillträdespunkten öppnas grinden. På så sätt förhindras obehöriga personer från att slinka genom den öppna grinden. Dessutom möjliggörs en smidig passage genom tillträdespunkten.



SNABBT TILLTRÄDE – ALLA GÅNGER

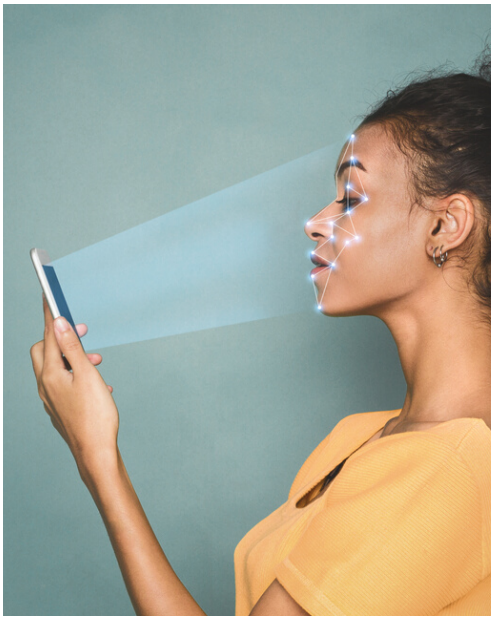
Biometrisk ansiktsigenkänning fungerar utifrån något man alltid bär med sig, därför behöver man inte oroa sig över dörrar som aldrig öppnas. Eftersom varje ansikte är unikt identifieras varje individ baserat på sina ansiktsdrag.

Ytterligare en fördel är att det endast krävs minimal användarinteraktion vid tillträdeskontrollpunkten. Så snart ett ansikte hamnar innanför kamerans fokusområde kontrollerar programvaran om tillträde ska godkännas. Eftersom passerkort inte längre är nödvändigt, behöver du heller inte oroa dig för att glömma eller förlägga ditt kort. Du behöver inte vänta på att en kollega ska leta fram sitt kort, och du har alltid händerna fria för att hålla i ytterplagg och väskor.

INGEN DELNING AV PASSERKORT

Ett vanligt problem inom tillträdeskontroll är att personliga passerkort delas med kollegor. Sådan felaktig användning kan leda till att obehöriga får tillträde till byggnaden. Ansiktsigenkänning förhindrar att obehöriga kan ta sig genom tillträdeskontrollen.

Och eftersom tillträdeskontroll via ansiktsigenkänning inte använder sig av passerkort, går det heller inte att stjäla eller kopiera ett kort. Resultatet är att den övergripande säkerheten förbättras.



BIOMETRISK KONTROLL SKER BERÖRINGSFRITT

Många personer tvekar en stund inför iris- eller fingeravtrycksavläsning. Denna tvekan beror (omedvetet) på att de är dåligt insatta i hur systemet fungerar eller att de känner olust inför att aktivt placera en kroppsdel nära avläsaren. Detta saktar ned flödet och kan leda till att tillträdeskontroll upplevs som mindre användarvänligt.

En annan stor fördel med ansiktsigenkänning är att användare registreras på avstånd med hjälp av en kamera. Användare behöver inte ställa sig i någon obekväm position eller röra vid tillträdespunkten. Så snart de hamnar innanför kamerans avkänningsområde, verifieras deras identitet och de kan avbrottsfritt fortsätta genom tillträdespunkten.

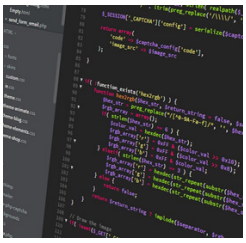
KOMPONENTER I ANSIKTSIGENKÄNNINGSTEKNIK.

När du funderar på att använda tillträdeskontroll via ansiktsigenkänning ska du även ta med de olika komponenterna som systemet består av i beräkningen. Dessa komponenter levereras ofta av olika parter som måste kunna interagera med varandra. Det är därför viktigt att kontrollera vilka leverantörer som tillsammans kan bygga upp ett smidigt fungerande system. I allmänhet ska följande komponenter kunna interagera med varandra:

KAMEROR OCH ANDRA SENSORER

Kameran är en viktig beståndsdel i ett tillförlitligt ansiktsigenkänningssystem. Det finns olika högkvalitativa kameror tillgängliga på marknaden. Det har visat sig att ett noggrant urval baserat på både tekniska och estetiska faktorer kan bidra till en mer användarvänlig och mindre obekväm upplevelse.

Det är inte bara kamerans megapixel som urvalet ska grundas på, ljuskänslighet, typ av lins och bearbetningskapacitet är också viktiga faktorer att tänka på. Det går även att lägga till ytterligare sensorer så att systemet kan skilja mellan ett ansikte och en bild.



ANSIKTSIGENKÄNNINGSPROGRAMVARA

Ansiktsigenkänningsprogramvaran kallas även för systemets hjärta. Den omvandlar ansiktsdrag till en kod som sedan jämförs med information i en databas. Igenkänning sker med hjälp av en serie algoritmer. Ansiktsigenkänningsprogramvaran fungerar ofta oberoende av andra tillträdeskontrollprogramvaror. På så sätt kan ett fristående system skapas där programvaran körs på en extern processor.

Det är viktigt att säkerställa att programvaran och systemet efterlever bestämmelserna i dataskydds-förordningen (General Data Protection Regulation, GDPR) samt använder korrekta krypteringsstandarder.

TILLTRÄDESKONTROLLSYSTEM

Tillträdeskontrollsystem använder ofta en kombination av olika programvarulösningar. Dessa lösningar integreras ofta med hjälp av ett säkerhetshanterings- eller byggnadshanteringssystem. Därför kan ansiktsigenkänningsprogramvaran även behöva vara kompatibel med ett sådant system.

I praktiken krävs även anslutning av olika moduler för efterföljande kontroll via ett enskilt centralt program. I sådant fall integreras ansiktsigenkänningsprogramvaran via en API.

FYSISKT TILLRÄDE

I tillträdeskontrolltillämpningar används ansiktsigenkänning alltid i kombination med fysisk tillträdeskontroll. Det är omöjligt att neka tillträde till obehöriga utan hjälp av någon slags barriär. Det finns olika barriäralternativ tillgängliga som alla har olika säkerhetsmässiga för- och nackdelar.

Det går att konfigurera komponenterna på olika sätt. Man kan till exempel få fysiska produkter med helt integrerad ansiktsigenkänning, men man kan även köpa komponenterna separat.

TEKNISKA ASPEKTER.

LJUSFÖRHÅLLANDEN

En av de viktigaste faktorerna för tillförlitlig ansiktsigenkänning är mängden ljus som finns på platsen där kameran är placerad. Tillträdeskontroll via ansiktsigenkänning sker ofta inomhus, vilket gör det enkelt att anpassa ljusförhållandena.

Överexponering kan vara en riktig utmaning. Det kan handla om starkt solljus, reflekterande bländande ljus och höga glastak. Skiftande ljusförhållanden kan vara svårt att hantera för kameror och programvaror.

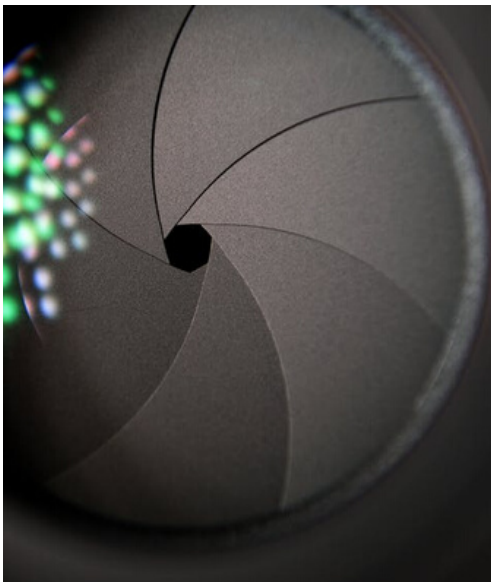
Underexponering är mycket lättare att korrigera. Ofta räcker det att justera kamerainställningarna för att korrekt identifiering ska kunna uppnås. Det är en god idé att låta en expert utföra dessa inställningar.

PLACERING AV KAMERAN

Vid montering av kameran är det viktigt att tänka på den registrerade bildens kvalitet. Ju närmare kameran befinner sig personen som ska kontrolleras, desto bättre blir bildens kvalitet.

Kamerans placering i förhållande till användaren är också viktigt. Det är bäst att placera kameran så att användaren redan står i riktning mot kameran när han eller hon ska passera genom tillträdespunkten. På så sätt slipper användaren ändra sin kroppsställning för att bli identifierad.

Av estetiska skäl är det även en god idé att integrera kameran i tillträdeskontroll-produkten eller montera den på en extern plats.



KAMERANS FOKUS

Kamerans fokus är också viktigt att tänka på vid montering av kameran. Fokus ska ställas in där ansiktsavläsningen sker. Fokusavståndet ska inte ligga för långt ifrån tillträdespunkten (för att förhindra att personer slinker förbi) och inte heller för nära (för att köbildning ska undvikas).

Kamerans fokus avgör även inom vilket omfång ansiktsigenkänning sker. Bildens ansiktsigenkänningsomfång väljs i programvaran.

Våra experter hjälper dig gärna att välja lämpliga tekniska specifikationer för just dina behov.

I PRAKTIKEN.

ANVÄNDARFLÖDE

I praktiken gör speedgates att användare naturligt intar en framåtriktad position. Användare rör sig genom produkten i en rak linje, vända framåt. Zonen inom vilken användarnas ansikte registreras är således relativt liten.

En annan fördel med tillträdeskontroll via ansiktsigenkänning är att användarflödet förbättras. Detta eftersom användarna rör sig i samma riktning genom speedgaten, i ett konstant flöde. Flödet upprätthålls eftersom autentisering sker tillräckligt snabbt.

ANSIKTSAVLÄSNING

Tidigare i denna guide nämndes att användare inte behöver ändra sin kroppsställning vid tillträdeskontroll via ansiktsigenkänning. Detta förutsätter emellertid att användaren är medveten om att programvaran måste kunna avläsa hans eller hennes ansikte.

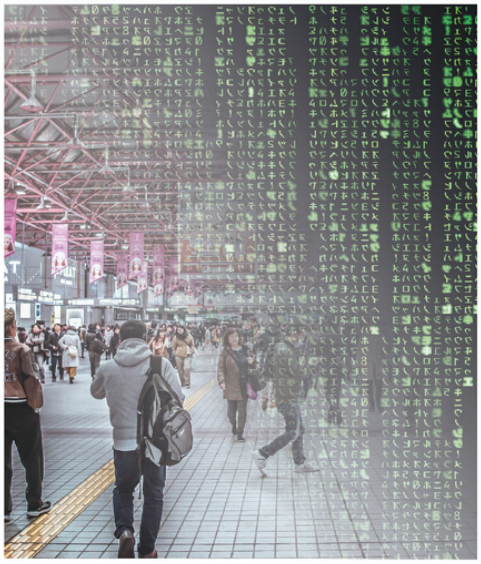
I praktiken innebär det att användare måste vara vända mot kameran utan att ansiktet döljs. De kommer inte att kunna passera tillträdespunkten om de till exempel bär en mask eller om de är vända bakåt. För att systemet ska fungera smidigt krävs samarbete från användarens sida.

ANVÄNDARINTERAKTION

När det gäller ansiktsigenkänning och tillträdeskontroll i allmänhet är det viktigt att användaren får god återkoppling. När en tillträdespunkt används av flera användare i snabb följd, kan bild- och ljudsignaler göra det lättare för användaren att uppfatta uppmaningar från programvaran.

Ansiktsigenkänning lämpar sig väl i situationer med många flergångsanvändare. Efter den första registreringen godkänns tillträde för användaren under den tid som krävs. Dessutom vänjer sig flergångsanvändare vid att interagera med tillträdeskontrollprodukten.

DIGITAL SÄKERHET.



KRYPTERING

För att förhindra att information och bilder som skickas över ett nätverk utsätts för hackning använder ansiktsigenkänningsprogramvaror kryptering. Kryptering innebär att digital information kodas. Krypterad information är omöjlig att läsa för utomstående eftersom man måste känna till vilken krypteringsmetod som har använts.

Det finns olika sätt att kryptera information. Vilken lösning som är mest lämplig beror på befintlig infrastruktur och aktuell programvaruplattform för video. Det spelar roll om till exempel information överförs via ett öppet nätverk eller ett slutet nätverk. Våra experter svarar gärna på frågor om detta ämne.

UPPTÄCKA BEDRÄGERI

När det gäller upptäckt av bedrägerier är ansiktsigenkänningsteknik i ständig utveckling. Målet är att förhindra att systemet ”vilseleds” genom att en bedragare till exempel visar upp ett kort mot kameran. Det finns i nuläget två sätt att upptäcka och förhindra bedrägeri:

- Maskinvarubaserad detektering där ansiktets struktur avläses via 3D-sensorer. Detta kan vara sensorer som registrerar mönstret hos färgade ljusstrålar som reflekteras mot ett ansikte.
- Programvarubaserad detektering som känner av väldigt små avvikelser i videobilden. För detta krävs stor videobearbetningskapacitet, vilket innebär större och mer kraftfulla servrar.

GDPR

Tidigare i denna guide nämndes att ansiktsigenkänningsteknik använder sig av biometrisk information. När det gäller dataskyddsförordningen (General Data Protection Regulation, GDPR) är det viktigt att känna till att biometrisk information tillhör en särskild kategori av personuppgifter. Information inom denna kategori får under vissa omständigheter användas för personidentifiering. Informationen får endast används i autentiserings- eller säkerhetssyften. Dessutom måste systemadministratören kunna bevisa att informationsbearbetning sker i enlighet med denna förordning. Ansiktsigenkänning inom tillträdeskontrollstillämpningar är därför tillåtet enligt lag.

SAMMANFATTNING.

Målet med denna guide är att erbjuda grundläggande insikt om tillträdeskontroll via ansiktsigenkänning och vad som omfattas i denna teknik samt vilka faktorer som avgör vilken lösning som lämpar sig mest för just din verksamhet. Skillnaderna mellan olika typer av biometriska metoder och ansiktsigenkänningsmetoder tydliggörs. Dessutom beskrivs fördelarna hos ansiktsigenkänning jämfört med traditionella tillträdeskontrollsystem.

Vi presenterar även de olika komponenterna i och de viktigaste tekniska och praktiska aspekterna hos tillträdeskontroll via ansiktsigenkänning. Slutligen beskrivs kortfattat hur ansiktsigenkänning behandlas inom digital säkerhet och aktuella GDPR-bestämmelser.

REKOMMENDATIONER

Med denna guide har Boon Edam [TG1] som mål att ge dig insikt i villkoren och kraven som är förknippade med ansiktsigenkänning. Vi anser att ansiktsigenkänningsteknik har bevisat sitt värde under de senaste åren och tror att användningen kommer att öka i framtiden. Vi vill dessutom understryka att ansiktsigenkänning är lämplig för tillträdeskontroll vid nästan alla säkerhetsnivåer. Baserat på dina önskningar vad gäller ansiktsigenkänningstillämpning och dina specifika omständigheter (till exempel antalet personer som ska identifieras, tillträdespunkt osv.) hjälper vi dig gärna att välja ut och implementera det mest optimala systemet för just dina behov.

Om du vill ha mer information om tillträdeskontroll via ansiktsigenkänning kan du kontakta våra entréexperter. Kontakta oss gärna för ett besök, utan bindningskrav.

VANLIGA FRÅGOR.

När jag som användare närmar mig en tillträdespunkt med ansiktsigenkänning så registreras mina ansiktsdrag och jämförs med information i en databas. Innebär det att även en bild av mig lagras?
Nej, databasen kräver inte lagring av användarens ansikte, endast en lista med hash-koder lagras. Tillträdeskontrollprodukter lagrar inte heller bilder i jämförelsesyften. Det kan emellertid hända att ansiktsigenkänningsprodukter (temporärt) lagrar bilder för optimering av programvaran. Dessa lagras i en fristående server och kan inte delas med tredje part.

Lagras någon annan information, förutom hash-koder?
Rent allmänt registrerar traditionella tillträdeskontrollsystem och ansiktsigenkänningssystem tiden då en behörig användare går in i en byggnad. Det går att justera inställningarna så att sådan information inte lagras.

Är denna typ av ansiktsigenkänning lämplig att använda ihop med andra entrélösningar, utöver spärrar?
Ja, denna typ av ansiktsigenkänning är lämplig att använda ihop med olika andra entrélösningar. Vi diskuterar gärna de olika möjligheterna med dig.

GLOBAL **NÄRVARO.**

Vi har varit verksamma i över 140 år. Vi tillverkar väldesignade entrélösningar av premiumkvalité i våra fabriker i Nederländerna, USA och Kina. Vi kan med säkerhet säga att vi täcker världens alla hörn med dotterbolag i stora städer över hela världen. Dessutom är vår globala exportavdelning inte bara leverantör till våra distributörer, utan kan också erbjuda direktförsäljning och service inom varje affärsområde. Detta breda nätverk gör det möjligt för oss att få en stark global närvaro samt ett personligt grepp om lokala marknader och deras unika krav på entrélösningar.

Kontakta din Boon Edam-expert på: www.boonedam.se

Boon Edam Sweden AB
T +46 (0) 8 753 60 30
E info@boonedam.se
I www.boonedam.se

BOON EDAM
YOUR **ENTRY** EXPERTS.