Numina sensors, een privacy by design oplossing.

Huidige wetgeving en privacy regels vragen om producten waarbij privacy deel uit maakt van de genen, producten waarbij beveiliging en privacy componenten zijn welke deel uitmaken van het volledige traject van product ontwikkeling tot levering en exploitatie.

De Numina sensoren zijn een ‘Privacy by Design’ oplossing. De sensoren verwerken data, met de nieuwste ‘edge computing’ technieken in de sensor zodat elk risico dat, naar personen te herleiden data bij gebruikers terecht komt wordt uitgesloten. In de sensor worden observaties gedaan binnen een statisch gebied. Er wordt geen data langdurig in opgeslagen data maar wordt slechts vluchtig gebruikt voor analyse met als doel object observaties te classificeren en alleen deze informatie voorzien van relatieve locatie en tijd.

De data die dit oplevert is ontdaan van alle context. Al in de sensor is deze dus niet meer naar personen te herleiden. De sensor stuurt data via een versleutelde verbinding door naar een beveiligde ‘IoT’ dataopslag die slechts vanuit een API en/of dashboards toegankelijk is voor geautoriseerde gebruikers. Ook hier wordt geen informatie verzameld welke te herleiden is naar personen.

Om de kwaliteit van de oplossing te kunnen borgen wordt met regelmaat een ‘snapshot’ gemaakt van de te observeren omgeving om de installatie de kunnen vrijgeven, observatie algoritmes te kunnen valideren en trainen en daarna via software te kunnen controleren en borgen op wijzigingen in de statische situatie van te observeren omgeving.

Deze ruwe data wordt slechts 30 dagen binnen de EU (AWS) opgeslagen. Software zorgt ervoor dat alleen snapshots waarbij personen onherkenbaar gemaakt zijn is in te zien door een gelimiteerd aantal geautoriseerde medewerkers. Hiervan wordt slechts incidenteel gebruik gemaakt bij falen van de automatische kwaliteitscontroles of noodzakelijk systeem onderhoud.

Betreffende medewerkers hebben ook toegang tot de minimale informatie inzake opdrachtgever en de door hen geautoriseerde gebruikers van dashboards en API. Voor dataopslag wordt gebruik gemaakt van het AWS platform conform de hiervoor geldende beveiligingsnormen en GDPR richtlijnen https://aws.amazon.com/compliance/data-center/controls/

Data is eigendom van de ‘producent’ veelal de ‘openbare ruimte’ en wordt niet ingezet voor eigen doelen anders dan verbetering van de producten en services. Dit wordt bevestigd in het privacy statement van Numina.

De sensoren zijn gefabriceerd conform ISO 9001. De integriteit van de sensoren en het back-end systeem is opgezet conform de IEC 62443 norm, een wereldstandaard welke een omkadering bieden voor de systeem integratie, beveiliging en lifecycle in relatie tot de toegepaste processen, personeel, hardware en software welke allen impact hebben op een veilige, betrouwbare en goed beveiligde werking. De sensoren garanderen de integriteit van de datastroom, samen met het Nederlands Meet Instituut (NMI) zijn we bezig met een certificering hiervan, deze is naar verwachting eind eerste kwartaal 2021 gereed.

Vermelde normen en werkwijze geeft een omkadering van doel en methode voor ‘Privacy Officer’ en / of onderbouwing voor een 'Data Protection Impact Assessment (DPIA)’.

Voor de klanten die meer informatie willen over de architectuur kunnen we detail info verstrekken na ondertekening van een NDA.

Intemo
Innovative Technology in Motion

Numina sensors, a privacy by design solution.

Current legislation and privacy rules require products in which privacy is part of the genes, products in which security and privacy are components that are part of the entire process from product development to delivery and exploitation.

The Numina sensors are a "Privacy by Design" solution. The sensors process data with the latest ‘edge computing’ techniques in the sensor making sure that any risk that data can be traced back to people reaches users is excluded. In the sensor observations are made within a static area. No data is long-term stored but is only used fleetingly for analysis with the aim of classifying object observations and providing them with relative location and time.

The data that this process produces will be been stripped of all context. Therefore, already in the sensor, it can no longer be traced back to people. The sensor forwards data via an encrypted connection to a secure "IoT" data storage that is only accessible to authorized users from an API and / or dashboards. Again no information is collected that can be traced back to persons.

To be able to guarantee the quality of the solution, a 'snapshot' of the environment is regularly made to be observed, in order to be able to release the installation, to validate and train observation algorithms and to be able to check and secure via software for changes in the static situation of the environment to be observed.

This raw data is only stored within the EU (AWS) for 30 days. Software ensures that only snapshots, in which people have been made unrecognizable, can be viewed by a limited number of authorized employees. This is only used incidentally in the event of failure of the automatic quality controls or in case of necessary system maintenance.

Concerned employees also have access to the minimum information regarding the client and their authorized users of the dashboards and API. For data storage the AWS platform is used in accordance with the applicable security standards and GDPR guidelines https://aws.amazon.com/compliance/data-center/controls/

Data is owned by the "producer", often the "public space" and is not used for own purposes other than improving the products and services. This is confirmed in Numina's privacy statement.

The sensors are manufactured in accordance with ISO 9001. The integrity of the sensors and the back-end system is set up in accordance with the IEC 62443 standard, a world standard that provides a framework for the system integration, security and lifecycle in relation to the applied processes, personnel, hardware and software which all have an impact on a safe, reliable and well-secured processing. The sensors guarantee the integrity of the data flow and we are working with the Netherlands Measurement Institute (NMI) to certify this, which is expected to be ready at the end of the first quarter of 2021.

Mentioned standards and working method provide a framework for the purpose and method for "Privacy Officer" and / or substantiation for a "Data Protection Impact Assessment (DPIA)".

For customers who want more information about the architecture, we can provide detailed information after signing an NDA.