IT Audit

ICT & Business - Atos

Proftaak project:	**Atos**	Projectleider:	**Roel van Zon**
Tutor:	**Sak, Ludo L.J.**	Projectleden:	**Mustafa Kaptan**
			Ivan Rimbow
Atos:	**Nick van Pelt**		**Willem Simonis**
	Bas Mommers	Versie:	**1.0**

INHOUD

INLEIDING

De afgelopen jaren worden steeds meer IT innovaties toegepast binnen het aanbod aan services van Atos. Atos focust zich veel op de continuïteit van de nieuwste technieken binnen het IT werkveld. Wanneer Atos het producten/services assortiment wilt uitbreiden, dan moet er nagedacht worden over hoe deze innovaties binnen dit aanbod kunnen worden geïmplementeerd. Daarbij is het belangrijk dat de bijbehorende risico's zoveel mogelijk vermeden worden en dat de implementatie geen schade zal opleveren aan Atos.

In dit document wordt een innovatie getoetst waarmee Atos haar klanten wilt gaan inspireren. De innovatie die getoetst zal gaan worden is een toepassing van sensoren op een Lego kraan. Deze kraan is gekoppeld aan het SAP IAM systeem met behulp van deze sensoren. De gegevens die zich binnen deze interfaces bevinden zullen onder andere bedrijfs-/kraan-/klant-/contactgegevens bevatten. Omdat deze privacy gevoelige gegevens zich in de gegevensstromen van deze innovatie bevinden, is het noodzakelijk om een Privacy Audit uit te voeren. Dit document is het resultaat van de uitvoering van de audit waaruit duidelijk wordt of de innovatie direct geïmplementeerd zou kunnen worden óf dat er eventuele maatregelen genomen moeten worden om de risico's te beperken.

PROBLEEMDEFINITIE EN CONTEXT

De laatste IT-ontwikkelingen binnen Atos hebben de mogelijkheid gegeven dat niet alle gegevens op een correcte manier worden behandeld. Omdat hier nog geen duidelijke/eenduidige procedure over bestaat is het nog niet mogelijk om de route van de gegevens exact te volgen. Door middel van een Privacy Audit uit te voeren op een van de laatste IT-ontwikkelingen (de Lego demo kraan), wordt gekeken naar het in gebruik nemen van bedrijfs- en persoonsgegevens en kunnen mogelijke risico's in kaart worden gebracht. Deze worden vergeleken met het normenkader van de AVG en het Privacy Control raamwerk. Dit is van belang om ervoor te zorgen dat de gegevens van het bedrijf en de medewerkers niet openbaar worden gesteld.

ONTWIKKELINGEN BINNEN ATOS EN BUSINESS CONSULTANCY

Op weg naar een digitale samenleving is Atos een sterke partner in transformatie, met veel aandacht voor analyse, engagement van de burger en cyberveiligheid. Al 30 jaar lang brengt Atos de voordelen van voortdurende innovatie naar veel verschillende klanten. Van overheidsinstellingen, van defensie tot onderwijs, van financiën tot gezondheidszorg. (Atos, sd)

Atos ontwikkelt zichzelf als bedrijf zijnde ook voortdurend op het gebied van innovatie. Zo zijn ze vanaf 2019 de samenwerking aangegaan met Fontys ICT Innovation Lab in Eindhoven. Atos is deze samenwerking aangegaan met het doel om met nieuwe innovatie te experimenteren en om deze innovaties te onderzoeken. Deze samenwerking heeft geleid tot een broedplaats voor innovatie, wat bij Atos op een aantal afdelingen al in gebruik wordt genomen. (Atos, 2019)

De consultancy tak wordt alsmaar breder en breder en de mogelijkheden worden steeds groter. Over het algemeen houden business consultants zich bezig met het in kaart brengen van de bedrijfsstrategie en de mogelijke problemen of bedreigingen die deze met zich meebrengen. Daarnaast laten de business consultants van Atos hun klanten zien wat zij kunnen bieden om deze problemen of bedreigingen op te lossen met een unieke & efficiënte oplossing.

AFBAKENING

In scope:

Voor het uitvoeren van een Privacy Audit wordt er getoetst op normenkaders door middel van het Privacy Control Framework. Zo valt het AVG, PCF en een gedeelte van de ISO27002 norm binnen de scope. Dit met betrekking tot het onderzoek naar de privacygevoelige informatie welke wordt verstuurd vanaf de sensor naar het doelsysteem. Zo zal er gewerkt worden met persoons- en bedrijfsgegevens van de klanten van Atos, die werkzaamheden verrichten met de Atos en de onderhoudsdienst.

DOEL

De reden waarom Atos een IT Privacy Audit gaat uitvoeren, is omdat Atos een mogelijke reputatieschade wil voorkomen wat uiteindelijk doelt op een verlies in de kosten. Om dit te onderzoeken hebben ze ondersteuning gevraagd aan Process Bulls.

Een IT-Audit is altijd gebaseerd op een bepaald criterium. Zo wordt er getoetst hoe volledig de informatie is die een systeem genereerd. Hierbij worden verschillende inzichten getoetst op basis van de betrouwbare informatie. Voor dit project is het gestelde criterium “Privacy”. Door de laatste IT-ontwikkelingen binnen Atos is het mogelijk dat niet alle gegevens op een correcte manier worden behandeld.

Door een Privacy Audit uit te voeren op de laatste IT-ontwikkelingen (de Lego demo kraan), wordt gekeken naar het gebruiken van bedrijfs- en persoonsgegevens en kunnen mogelijke risico’s in kaart gebracht worden. Hierbij worden deze vergeleken met de kwaliteitseisen vanuit het normenkader.

ONDERZOEKSOPZET

ONDERZOEKSVRAGEN

De opzet van het onderzoek bestaat uit een hoofdvraag met daarbij enkele deelvragen. Om de hoofdvraag te kunnen beantwoorden, zullen we eerst de deelvragen moeten beantwoorden. Om het beoogde eindresultaat te behalen hebben we diverse instrumenten nodig. Een grote rol hierin hebben de docenten. Zij zijn een bron van informatie en feedback op de opgeleverde producten. Daarnaast gebruiken wij het internet om andere bronnen en informatie te vinden, ook om vergelijkbare projecten/bedrijven op te zoeken.

Hoofdvraag

Hoe voldoet de gegevensstroom van Atos tussen de sensoren tot aan het doelsysteem, welke bedrijfs-/kraan-/klant-/contactgegevens bevat, aan de privacy normenkaders?

Deelvraag

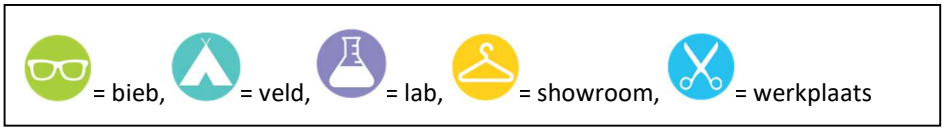
1. Hoe worden de normenkaders gebruikt bij de Privacy Audit?
2. Welke gegevens worden gebruikt met betrekking tot de privacywetgeving?
3. Wat zijn de risico's wanneer de gegevensstroom tussen de sensoren en het SAP IAM niet correct worden verstuurd?

ONDERZOEK METHODIEK

Deze audit is gebaseerd op een onderzoek. Om dit onderzoek valide te laten zijn, worden de onderzoeksvragen vanuit verschillende perspectieven benaderd. In dit onderdeel van het document wordt de onderzoeksopzet verder beschreven en de aanpak van het project.
Wij hanteren het DOT framework als onderzoeksmethodiek tijdens deze audit. De benadering van de deelvragen zijn gespecificeerd in tabel 1. In de rechterkolom staat weergeven welke onderzoeksmethodieken er zijn gebruikt, in de vorm van triangulatie, om antwoorden te verwerven. Hieronder zijn de onderzoeksmethodes in het kort toegelicht:

Showroom: In deze fase wordt er een feedback/beoordeling plaats gevonden op het onderzoeksrapport;
Literatuurstudie: In deze fase wordt er gekeken naar de eventuele bronnen die op het internet te vinden is;
Veldonderzoek: In deze fase worden de professionals geïnterviewd om beter inzicht te krijgen in een bepaalde vraagstukken.

Daarnaast zijn de andere onderzoeksmethodes niet relevant binnen het project.



Figuur 1 Legenda onderzoekstrategie

Deelvraag	Onderzoeksmethodiek
1. Hoe worden de normenkaders gebruikt bij de Privacy Audit?	
2. Welke gegevens worden gebruikt met betrekking tot de privacywetgeving?	
3. Wat zijn de risico's wanneer de gegevensstroom tussen de sensoren en het SAP IAM niet correct worden verstuurd?	

Tabel 1 Onderzoeksvragen met strategieën

- Resultaten & Analyse -

”

“Hard werken om een goed resultaat te behalen”

Atos

WELKE GEGEVENS WORDEN GEBRUIKT MET BETREKKING TOT DE PRIVACYWETGEVING?

WAT IS DE PRIVACYWETGEVING?

De privacywetgeving dient ter bescherming van persoonsgegevens. Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De AVG vervangt Wet Bescherming Persoonsgegevens (WBP) en geldt in de hele Europese Unie (EU). Het doel van de Verordening is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de EU. Deze handleiding van de AVG beschrijft wat deze wetgeving betekent voor partijen die persoonsgegevens verwerken en aan welke regels de gegevensverwerking moet voldoen. (Bart W. Schermer, Dominique Hagenauw, Nathalie Falot, 2018)

HOE WORDT DE PRIVACYWETGEVING GETOETST?

De AVG-handleiding, gepubliceerd door de rijksoverheid, kan helpen om erachter te komen welke gegevens er worden verwerkt bij de Lego Demo Kraan. Deze handleiding bestaat uit de belangrijkste bepalingen uit de uitvoeringswet van de AVG en is in het bijzonder bedoeld voor lezers die reeds enigszins op de hoogte zijn van het gegevensbeschermingsrecht en op zoek zijn naar verdere verdieping. Zo kan men de maatregelen binnen hun organisaties, die bij de verordening vereist zijn, implementeren. In hoofdstuk 3 uit de Handleiding Algemene Verordening Gegevensbescherming (zie Bijlage II) staat een reeks vragen genoteerd waardoor vastgesteld kan worden of de AVG van toepassing is en welke gegevens daarbij komen kijken. Deze vragen zijn beantwoord en staan in Bijlage III weergeven.

BEVINDINGEN

Uit de beantwoording van deze vragen blijkt het volgende:

- De Lego Demo Kraan zelf voldoet aan de eisen van de AVG wet. Bij deze demo is SAP de verwerkingsverantwoordelijke aangezien Atos de klantgegevens bij de demonstratie niet in een apart document borgt.
- Indien een klant de Lego Demo Kraan toepast in de praktijk, dan moet deze klant zich het volgende afvragen indien het de klantgegevens in een apart document borgt:
    1) Zijn de persoonsgegevens die verwerkt worden van organisaties (en personen) die in de EU zijn gevestigd en/of zijn deze persoonsgegevens van organisaties (en personen) die niet in de EU zijn gevestigd, maar wel gegevens verwerken van burgers in de EU?
    2) Indien “ja” dan geldt de AVG wet voor de klant en moet het de gegevens van de organisatie en/of personen die erbij komen kijken ieder moment kunnen verwerken als verwerkingsverantwoordelijke.

De persoonsgegevens die bij de Lego Demo Kraan worden gebruikt met betrekking tot de privacywetgeving zijn:

- Bedrijfsgegevens van het kraanbedrijf (bedrijfsnaam, locatie). Deze stromen van de NXT Brick naar het SAP-platform.
- Persoonsgegevens van de Business Partners (naam, e-mail, telefoon, adres, postcode, plaats). Deze stromen van en naar het SAP-platform naar de voorbeeldapplicatie.

HOE WORDEN DE NORMENKADERS GEBRUIKT BIJ DE PRIVACY AUDIT?

WELKE NORMENKADERS WORDEN ER GEBRUIKT BIJ EEN PRIVACY AUDIT?

Binnen een Privacy Audit kunnen er meerdere normenkaders worden toegepast, maar vanuit Process Bulls gaan er drie verschillende normenkaders gebruikt worden. Hierbij gaat het om de AVG (Algemene Verordening Gegevensbescherming), het Privacy Control Framework en ISO27002.
De verschillende normenkaders en het gebruik hiervan zullen hieronder beschreven worden.

AVG

WAT IS DE AVG?

De AVG staat voor Algemene Verordening Gegevensbescherming en geldt in de gehele Europese Unie, ook wel GDPR genoemd. De AVG zorgt voor de bescherming van persoonsgegevens door middel van verschillende richtlijnen. Door de introductie van deze Europese wet zijn er meer controles gekomen op het gebruik en misbruik van persoonsgegevens. Dit is bedoeld als vervanger van de Wet bescherming persoonsgegevens. De AVG kan gebruikt worden in combinatie met het Privacy Control Framework en hierbij wordt verwezen naar een citaat uit het NOREA boek. Het citaat is te vinden in de bijlagen.

WELKE GEGEVENS WORDEN ER ALS DATA GETRANSPORTEERD?

Binnen de nieuwe processen zijn er verschillende gegevens welke worden en hiervoor dient er eerst gekeken te worden naar welke gegevens van belang zijn. Er zal op de volgende manier data getransporteerd worden vanuit de Lego kraan sensor naar SAP IAM.

De realtime gegevens vanuit de kraan sensoren:

- De sensor op de kraan geeft realtime gegevens door aan het hoofdbord van de kraan;
- Het hoofdbord geeft de realtime gegevens door aan SAP PAI;
- SAP PAI laat de gegevens naar de verschillende onderdelen van het SAP IAM systeem;
- SAP IAM geeft in het klant portaal de realtime gegevens weer.

De bedrijfsgegevens:

- Het hoofdbord is gekoppeld aan een kraan en aan een klant;
- De realtime data wordt met de klant-/bedrijfsgegevens verstuurd naar de NXT Brick;
- De gegevens worden vanuit NXT Brick naar SAP PAI gestuurd;
- SAP PAI laat de gegevens naar de verschillende onderdelen van het SAP IAM systeem;
- SAP IAM geeft in het klant portaal de realtime gegevens weer.

WORDEN ER GEGEVENS OPGESLAGEN? ZO JA, HOE LANG?

Binnen de nieuwe innovatie zullen er meerdere gegevens worden getransporteerd en worden opgeslagen. Deze gegevens zijn gebonden aan de AVG-wetgeving en dit houdt in dat deze gegevens alleen bewaard mogen blijven wanneer deze nodig zijn om taken uit te voeren. Om persoonsgegevens te verwerken dient er een grondslag voor te zijn en deze dienen verwerkt te worden in de privacyverklaring, privacy beleid en mogelijk in het verwerkingsregister. Er dient zelf bepaald te worden welke van de zes verschillende grondslagen van toepassing is voor het verwerken van de persoonsgegevens.

De zes grondslagen zijn als volgt: (Mag u persoonsgegevens verwerken?, sd)

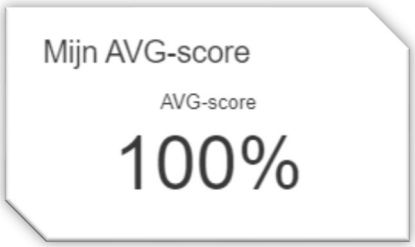
- U heeft toestemming van de persoon om wie het gaat.
- Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
- Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent.
- Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
- Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
- Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen.

De gegevens welke in het gehele proces opgeslagen worden zijn als volgt:

- Type sensor;
- Type kraan;
- Positie van de sensor;
- Kraan eigenaar;
- Contactgegevens van de kraan eigenaar;
- Contactgegevens van het onderhoudsteam;
- Data connectie tussen het hoofdbord en SAP IAM.

CHECKLIST RESULTATEN

In de AVG check is uitgekomen dat Atos volledig AVG proof is op het gebied van Informatiebeveiliging. De gehele check is vindbaar zijn in de bijlage vanwege de grootte van het document.



ISO27002

WAT IS ISO27002?

ISO27002 is een onderdeel vanuit het informatiebeveiligingsnormenkader. ISO27002 is een verdieping op de ISO27001 norm en het is een hulpmiddel om een risicoanalyse uit te voeren. ISO27002 bestaat uit verschillende maatregelen waarmee je bepaalde risico's kunt analyseren en beperken/verkleinen m.b.t. de informatiebeveiliging.

De ISO27002 norm bestaat uit veel verschillende controles die zijn ontworpen om een verdieping te geven op de ISO27001 norm en de mogelijkheid bieden om geïmplementeerd te worden.

WAT WORDT ER TIJDENS DE AUDIT GEDAAN MET ISO27002?

Tijdens de audit op de privacy wordt er gekeken naar meerdere categorieën binnen de informatiebeveiliging. Hierin zal er gekeken worden naar de onderstaande onderdelen: (Tsigkou, 2021)

Intellectueel eigendom

De betrokken partijen aanvaarden dat de intellectuele eigendomsrechten met betrekking tot alle software of andere materialen zoals analyses, ontwerpen, documentatie, rapporten, offertes en alle voorbereidende materialen die door of namens een partij aan de andere partij worden verstrekt in het kader van de overeenkomst, bij de uitgevende partij blijven.

Zie ook: NEN-ISO/IEC 27002:2013 sub-sectie 18.1.2

Vertrouwelijkheid

De betrokken partijen zijn bereid om een geheimhoudingsovereenkomst te sluiten. Deze overeenkomst bepaalt hoe informatie met betrekking tot de dienst(verlening) of het product zal worden behandeld en/of wordt verwerkt. De overeenkomst bepaald eveneens de sancties die kunnen worden toegepast als er sprake is van het niet nakomen van een of meerdere bepaling zoals opgenomen in de overeenkomst. Op verzoek zullen beide partijen een toelichting krijgen op de wijze waarop de andere partij zich aan deze bepaling(en) houdt.

Zie ook: NEN-ISO/IEC 27002:2013 sub-sectie 13.2.4

Beleid

De leverancier kan aantonen dat het personeel dat hij in dienst heeft, in staat is om de opdracht uit te voeren. De leverancier kan tevens aantonen dat zijn of haar personeel beschikt over de juiste trainingscertificaten, om de in de overeenkomst gespecificeerde dienst of product correct te kunnen leveren.

De leverancier kan aantonen dat het personeel, dat is ingeschakeld om de opdracht uit te voeren, een zorgvuldig screeningproces heeft ondergaan. De leverancier garandeert dat het personeel dat belast is met de uitvoering van de opdracht, zich ertoe zal verbinden om zich te houden aan en zich te gedragen in overeenstemming met het informatiebeveiligingsbeleid van de klant. De klant verstrekt de leverancier indien nodig vooraf een kopie hiervan ter beoordeling.

Zie ook NEN-ISO/IEC 27002:2013 sub-sectie 15.1.2 (i, l, p)

Auditing

De leverancier stemt ermee in om de klant toe te staan, het proces en de resultaten van de overeenkomst te controleren of te laten controleren door middel van een (externe) informatiebeveiligingsaudit. Tussen de partijen worden afspraken gemaakt over de datum, het tijdstip, door welke partijen, welke partij de kosten draagt (inclusief distributie) en tegen welke kosten de audit zal worden uitgevoerd.

Zie ook: NEN-ISO/IEC 27002:2013 sub-sectie 15.2.1

Rapportage

De leverancier heeft een proces geïmplementeerd waarin informatiebeveiligingsincidenten en risico's met betrekking tot de uitvoering van de opdracht, worden gerapporteerd en effectief worden afgehandeld. De leverancier is bereid dit proces indien nodig te laten inspecteren.

Zie ook: NEN-ISO/IEC 27002:2013 sub-sectie 16.1.2 & 16.1.3

CHECKLIST RESULTATEN

In tabel 2 staan de bevindingen weergeven van de ISO27002 check. De uitwerking van deze checklist is terug te vinden in Bijlage V. De resultaten laten zien in hoeverre de innovatie momenteel voldoet aan de ISO2007 checklist. Ook wordt er aangegeven aan welke onderdelen uit de ISO27002 nog met aandacht naar gekeken dient te worden voordat de innovatie wordt geïmplementeerd. De onderdelen konden namelijk nog niet met zekerheid afgevinkt worden.

Categorie binnen de informatiebeveiliging	Check	Onderdelen waar nog met aandacht naar gekeken dient te worden
Intellectueel eigendom	7/12	C, D, H, I, L
Vertrouwelijkheid	7/10	E, F, J
Beleid	8/16	C, D, H, I, L
Auditing	3/8	A, B, E, G, H
Rapportage	6/8	A, E
Totaal	31/54 = **57,4%**	

Tabel 2 ISO27002 score

Om te voldoen aan de ISO27002 normering, dient er nog aandachtig gekeken te worden naar de onderdelen uit tabel 2. Momenteel voldoet de toepassing van de innovatie voor **57,4%** met zekerheid aan de ISO27002 informatiebeveiliging normering.

PRIVACY CONTROL FRAMEWORK

WAT IS HET PRIVACY CONTROL FRAMEWORK?

Het Privacy Control Framework (hierna: 'PCF') uiteengezet dat is ontwikkeld door NOREA (de Nederlandse beroepsorganisatie van gekwalificeerde IT-auditors/ Nederlandse Orde van Register EDP-auditors).

Het primaire doel van het PCF is het bieden van ondersteuning aan (audit)professionals bij de beoordeling of de beheersingsdoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden behaald. Het PCF kan worden gebruikt als startpunt voor privacy audits op maat. Het PCF bevat de voorgeschreven beheersingsdoelstellingen en voorbeelden van maatregelen voor privacy opdrachten op basis van de NOREA Richtlijn 3000. Het PCF kan eveneens worden gebruikt om invulling te geven aan het privacy-deel van een SOC 2® Assurance rapport voor een entiteit die moet voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Het PCF kan daarnaast door entiteiten worden gebruikt om vast te stellen of de maatregelen ten aanzien van privacybescherming adequaat zijn, of om te bepalen in hoeverre de huidige maatregelen dienen te worden aangepast om te voldoen aan (wijzigingen in) wetgevingskaders (zoals de AVG).

Het PCF is gebaseerd op een informatielevenscyclusmodel, waarbij de volgende 'best practice' raamwerken in ogenschouw werden genomen:

- GAPP - gepubliceerd door de AICPA/CICA;
- NIST SP800-R53 Privacy Control Catalog;
- NOREA Raamwerk Privacy Audit;
- EuroPriSe raamwerk.

Voor elke fase is bepaald welke privacy onderwerpen van toepassing zijn. Deze onderwerpen worden weergegeven door middel van een afkorting van drie letters (32 in totaal). Elk privacy onderwerp is gekoppeld aan een beheersingsdoelstelling en deze is vervolgens vertaald naar een aantal beheersingsmaatregelen die dienen te worden geëvalueerd (95 in totaal). Deel 2 biedt een overzicht van de privacy onderwerpen en de hieraan gerelateerde beheersingsdoelstellingen. Deel 3 bevat een gedetailleerde lijst met de beheersingsmaatregelen per onderwerp. (NOREA, 2019)

TOEPASSING VAN HET PRIVACY CONTROL FRAMEWORK

Bij de beoordeling van de privacy beheersingsmaatregelen kan de IT-auditor het PCF gebruiken als een algemeen toetsingskader en dit aanpassen aan scope van de beoordeling. Het is daarbij goed om eerst de privacy onderwerpen en de hieraan gerelateerde beheersingsdoelstellingen in deel 2 van het PCF door te nemen en daarna een selectie te maken op basis van de scope van de opdracht. Vervolgens kan voor de geselecteerde onderwerpen en doelstellingen worden bepaald welke beheersingsmaatregelen uit deel 3 dienen te worden beoordeeld. Het is tot slot aan de IT-auditor om de beheersingsmaatregelen zodanig te wijzigen of aan te scherpen dat deze zo goed mogelijk zijn afgestemd op de scope en het doel van de opdracht. (NOREA, 2019)

WAT ZIJN DE RISICO'S WANNEER DE GEGEVENSSTROOM TUSSEN DE SENSOR EN SAP IAM NIET CORRECT WORDEN VERSTUURD?

Het functioneren van de communicatie tussen verschillende onderdelen van een bedrijf is van essentieel belang. Wanneer deze gegevensstroom niet soepel verloopt kunnen er zich allerlei risico's voordoen.

Atos is een bedrijf dat zich op het gebied van de ICT blijft ontwikkelen en constant opzoek is naar nieuwe innovatieve ideeën. Bijvoorbeeld bij de communicatie tussen de geleverde kranen en het SAP-systeem binnen Atos. Op de kranen bevinden zich verschillende sensoren die informatie over de kranen doorsturen naar SAP, zo weet het bedrijf wanneer de kraan bijvoorbeeld onderhoud nodig heeft of wanneer er iets defect is. Door deze innovatieve ideeën trekt Atos meer klanten aan. Het is natuurlijk wel belangrijk dat dit systeem goed functioneert, en wanneer dit niet zo is kunnen er verschillende risico's optreden.

RISICOANALYSE

Door vroegtijdig de risico's, gevolgen en de acties om het risico te beperken te inventariseren wordt het mogelijk om de risico's te beheersen en te monitoren gedurende het project. Tevens wordt het hierdoor duidelijk hoe er met de verschillende risico's wordt omgegaan. De risicoanalyse wordt beoordeeld door de **Kans x Impact**.

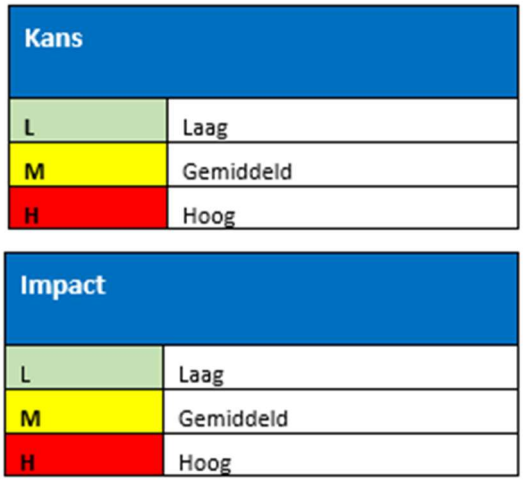
UITLEG LEGENDA

- **Een laag risico**
  - Wanneer er een onderdeel een laag risico heeft, wilt dat zeggen dat het probleem momenteel nog niet veel impact zal hebben op het bedrijf. Een voorbeeld zou kunnen zijn dat de gebruiksvriendelijkheid van de onderhoudsapp niet leesbaar is voor alle medewerkers.

- **Gemiddeld risico**
  - Wanneer er sprake is van een gemiddeld risico, is het belangrijk om te kijken wat het probleem is. Dit zal kunnen oplopen tot hoog risico, indien dit wordt uitgesteld.

- **Hoog risico**
  - Bij een hoog risico is het belangrijk dat er gelijk gehandeld wordt. Een hoog risico zal in de meeste gevallen schade brengen aan het bedrijf.

Kans		Risico
HxH	H	Hoog
HxL	M	Gemiddeld
HxM	H	Hoog
LxH	M	Gemiddeld
LxL	L	Laag
LxM	L	Laag
MxH	H	Hoog
MxL	L	Laag
MxM	M	Gemiddeld



Figuur 2 Legenda kans en impact

#	Risico	Omschrijving	Kans	Impact	Risico	Maatregelen
1	Sensor kan niet communiceren met SAP	Wanneer de sensoren constateren dat de kraan niet goed werkt en dus onderhoud nodig heeft moeten ze dit kunnen doorgeven aan het SAP-systeem zodat dit onderhoud geregeld kan worden. Wanneer deze gegevens niet correct aankomen bij het SAP-systeem kan het voorkomen dat er doorgewerkt wordt met een kraan die reparaties en onderhoud had moeten krijgen.	M	H		• De kraan dient direct buiten werking gesteld te worden; • De kraan moet handmatig gecontroleerd worden zodat het bedrijf een monteur kan inschakelen. • De kraan moet een periodieke controle krijgen los van de door sensoren aangegeven defecten zodat ze altijd gecontroleerd worden ook al werkt het systeem niet;
2	Vrijkomen van privacy gevoelige informatie	Met oog op de AVG-wetgeving en het respecteren van de privacy van (in)direct betrokkenen dient er rekening gehouden te worden met privacy.	M	H		• Zorg voor overzicht op de situatie. • Neem onmiddellijk maatregelen om de schade van het datalek te beperken. En schat de risico's in. • Bepaal of u het datalek wel of niet moet melden aan de Autoriteit Persoonsgegevens (AP). Zo ja, doe dit onmiddellijk. • Bepaal of u het datalek wel of niet moet melden aan de betrokken personen. Zo ja, doe dit zo snel mogelijk. • Registreer het datalek in uw datalekregister.
3	Sensor defect	De sensor is defect en hierdoor kan de klant niet uitlezen wat de status hiervan is.	L	H		• Monteur dient met spoed de sensor te vervangen; • Kraan dient buitenwerking gesteld worden; • Contact met klant opnemen over mogelijk defect;
4	Storing in SAP	Door een storing binnen het SAP-systeem is het niet mogelijk om data hierin te schrijven en uit te lezen.	L	H		• Contact opnemen met SAP-contactpersoon; • Contact opnemen met klant; • Aangeven dat doorwerken op eigen risico is; • Controleer groene boek voor mogelijk onderhoud bij echte kraan;
5	Uitstel onderhoud	Het onderhoud wordt vertraagd door een eventuele storing tussen het SAP-systeem en de gebruikende partij.	L	M		• Het bedrijf moet transparant zijn tegenover de klant en aangeven wanneer er vertraging optreedt; • Het bedrijf moet genoeg voorraad hebben zodat onvoorziene reparaties snel uitgevoerd kunnen worden.

Tabel 3 Risico met maatregelen

DISCUSSIE

Voor dit onderzoek heeft Process Bulls 3 een Privacy Audit uitgevoerd. Hierbij zijn 3 deelvragen opgesteld waarbij elk deelvraag een antwoord geeft op de volgende hoofdvraag:

"*Hoe voldoet de gegevensstroom van Atos tussen de sensoren tot aan het doelsysteem, welke bedrijfs-/kraan-/klant-/contactgegevens bevat, aan de privacy normenkaders?"*

Atos zit nog in een innovatietraject, waardoor het lastig te peilen is wat er specifiek geaudit moet worden. De klant moet zelf gaan peilen in hoeverre de privacy audit valide is. De audit die momenteel uitgevoerd is, is op basis van hoe de studenten de audit zouden aanpakken. Hiervoor hebben zij gebruik gemaakt van het ISO27002 en het PCF in combinatie met de AVG.

De resultaten van deze audit is onderbouwd door middel van de toepassing van het DOT Framework en zijn terug te vinden in de bijlage.

Voor het toetsen van de ISO27002 normering zijn niet alle onderdelen gebruikt. Zo is er niet gekeken naar de volgende onderdelen: Middelen, Regels en voorschriften, Subcontracting, Toegang en Reporting. Deze onderdelen zijn niet inbegrepen binnen de Privacy Audit in verband met dat deze onderdelen niet relevant zijn binnen het innovatie project.

CONCLUSIE & AANBEVELING

Uit dit onderzoek is gebleken dat Atos grotendeels voldoet aan de gehanteerde normenkaders voor het Privacy Audit. Bij het beoordelen van de ISO27002 norm komt er een resultaat van **57,4%** uit. Dit is berekend op basis van de 54 punten die getoetst zijn en de uitkomsten hiervan.

De studenten hebben deze Privacy Audit getoetst door middel van een, door NOREA opgestelde, checklist. De relevante aandachtspunten binnen de Privacy Audit zijn door middel van de checklist naar voren gekomen en hierop is een conclusie over het innovatie project aangeleverd.

Aanbeveling AVG

Uit het onderzoek is gebleken dat Atos voldoende scoort binnen de AVG van het innovatie project. Dit komt doordat aan alle getoetste onderdelen binnen de informatiebeveiliging wordt voldaan. Hierbij is het wel van belang dat er ten allertijden transparant naar de klant wordt gecommuniceerd welke gegevens er worden gebruikt voor welk doeleind.

Aanbeveling ISO27002

Binnen de ISO27002 toetsing heeft Atos een score behaald van **57,4%** en hieruit kan geconcludeerd worden dat er ruimte is voor verbetering binnen het innovatie project. Hierbij wordt aanbevolen dat er meer aandacht naar de ISO27002 toetsing om hiervoor het informatiebeveiligingscertificaat te behalen.

Conclusie

Na het uitvoeren van de gehele IT Privacy Audit kan er geconcludeerd worden dat er, binnen dit innovatie project, voldaan wordt aan de Privacywetgeving AVG maar de score van ISO27002 te laag is. Hier dient meer aandacht aan besteed te worden om zo een veilige innovatie neer te zetten en toekomst bestendig te werk te kunnen gaan.

BRONNEN

Atos. (sd). Opgehaald van Atos: https://atos.net/en/

Atos. (2019, 3 4). *Atos sluit zich als partner aan bij Fontys ICT InnovationLab in Eindhoven*. Opgehaald van Atos: https://atos.net/nl/2019/persberichten_2019_03_04/atos-sluit-zich-als-partner-aan-bij-fontys-ict-innovationlab-eindhoven

Bart W. Schermer, Dominique Hagenauw, Nathalie Falot. (2018). *Handleiding Algemene verordening gegevensbescherming (AVG).* Ministerie van Justitie en Veiligheid.

Checklist. (sd). Opgehaald van Aspect ICT: https://www.aspect-ict.nl/checklist

Mag u persoonsgegevens verwerken? (sd). Opgehaald van Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken

NOREA. (2019). *NOREA Handreiking Privacy Control Framework.* Amsterdam: NOREA.

Privacywetgeving AVG, wat moet je ermee? (sd). Opgehaald van https://www.kvk.nl/advies-en-informatie/wetten-en-regels/privacywetgeving-avg-wat-moet-je-ermee/.

SAP. (2011). *IAM100 - SAP Intelligent Asset Management Overview.* SAP.

SAP. (2021). *IAM100 - SAP Intelligent Asset Management Overview .*

Tsigkou, A. (2021, 01 14). *ISO 27002 checklist*. Opgehaald van ISO2HANDLE: https://www.iso2handle.nl/iso-27002/iso-27002-checklist/

FIGUURLIJST

TABELLEN

FIGUREN

BIJLAGEN

BIJLAGE I: CITAAT PRIVACY CONTROL FRAMEWORK EN DE AVG

De beheersingsdoelstellingen en de voorbeelden van maatregelen in het PCF sluiten nauw aan bij en zijn gekoppeld aan 13 kernelementen van de AVG. De kernelementen zijn geselecteerd op basis van een deskundig oordeel en de onderwerpen in het document 'In 10 stappen voorbereid op de AVG' van de Autoriteit Persoonsgegevens. Wanneer een entiteit de volledige set PCF-criteria hanteert, dient men deze hoofdonderwerpen van de AVG te behandelen en maatregelen te treffen om de van toepassing zijnde wettelijk verplichte doelstellingen te behalen.
Met de implementatie en uitvoering van de maatregelen kan met een redelijke mate van zekerheid gewaarborgd worden dat de beheersingsdoelstelling waartoe die maatregelen behoren wordt behaald. Hoewel de beheersingsdoelstellingen en -maatregelen in het PCF aansluiten op de beginselen van de AVG, biedt het toepassen van het PCF niet de garantie dat ook volledig aan de vereisten uit de AVG wordt voldaan. De AVG is een veelomvattende wet die tal van gedetailleerde vereisten voor specifieke situaties bevat. Met het oog op de praktische toepasbaarheid van het document worden deze vereisten niet allemaal in het PCF behandeld. Professionals die de privacy maatregelen van een entiteit beoordelen (bijvoorbeeld door via een gapanalyse vast te stellen of de entiteit aan de eisen van de AVG voldoet) wordt aangeraden aanvullende bronnen te gebruiken bij de identificatie en naleving van de specifieke wettelijke vereisten (zoals de Uitvoeringswet AVG) en gezaghebbende leidraden (zoals van de European Data Protection Board, EDPB) die op de betreffende entiteit van toepassing zijn.

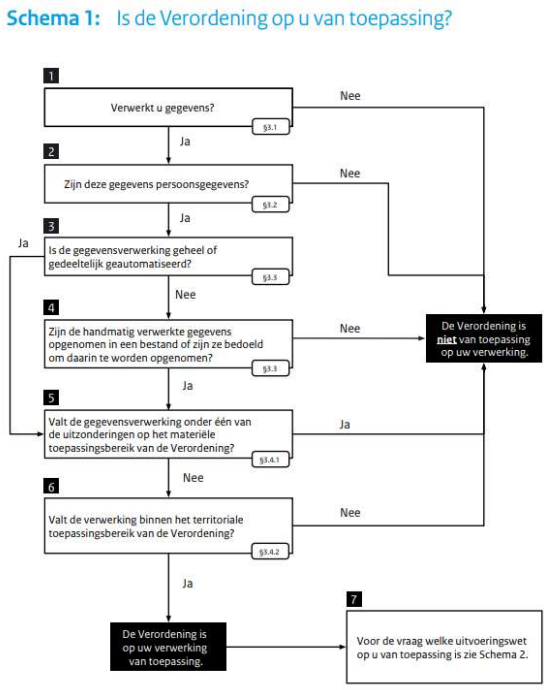
De verschillende relaties zijn zichtbaar in het bijgevoegde pdf-document.

Relatie AVG PCF.pdf

BIJLAGE II: HANDLEIDING AVG

Handleiding+Algemene+verordening+geg

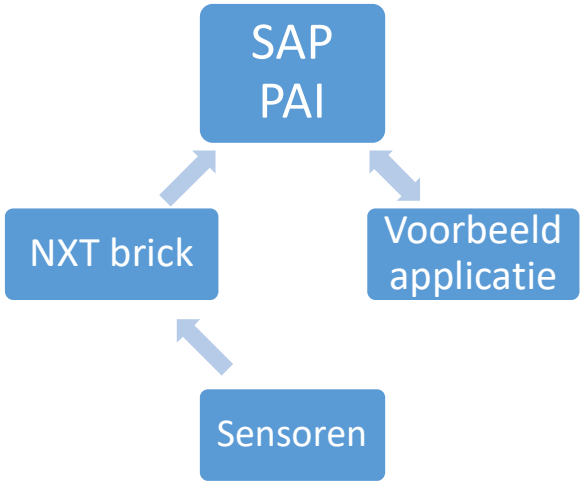
BIJLAGE III: BEANTWOORDING VRAAGSTUKKEN



Figuur 3 AVG proces

1. *Verwerk ik gegevens?*

Ja:

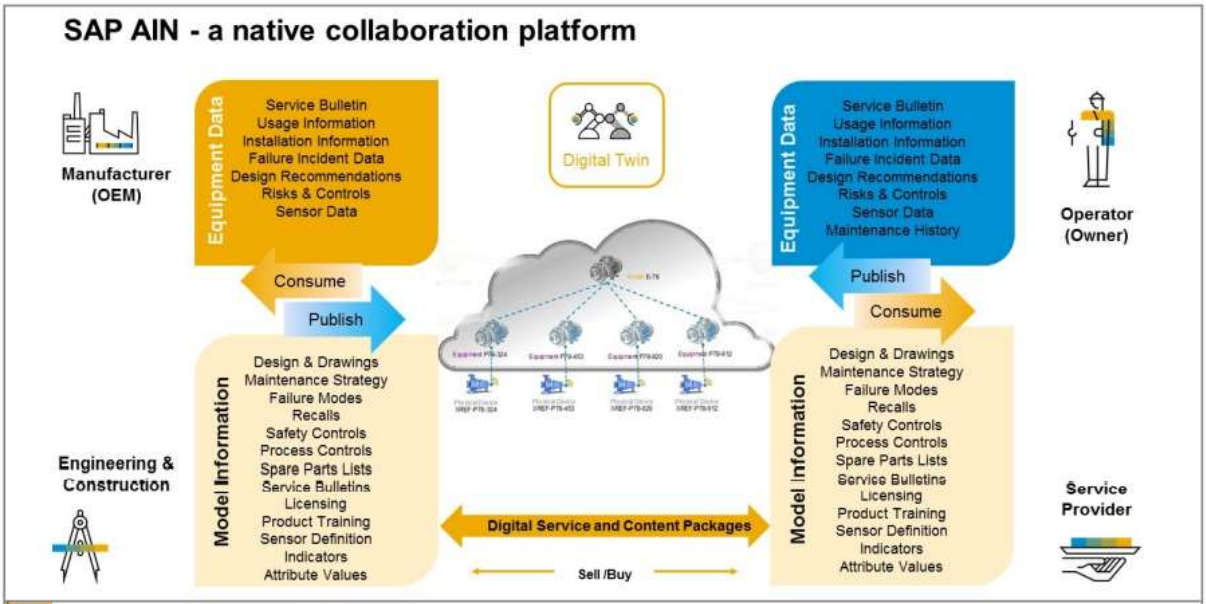


Figuur 4 Gegevensstroom

2. Zijn deze gegevens persoonsgegevens?

“De interfaces bestaan uit 3 gegevensstromen:

- Gebruiksgegevens van de sensoren naar de NXT Brick device;
    - De drukgegevens vanuit de sensor naar het ontvangende systeem gestuurd.
- De gegevensstroom van de NXT Brick naar de SAP AIN/PAI omgeving (de NXT Brick dient hierbij als gateway);
    - De druk- en bedrijfsgegevens worden vanuit het NXT Brick naar SAP AIN/PAI gestuurd. Dit bevat de gegevens over de kraan, het bedrijf dat de kraan gebruikt en wat de huidige sensor output is.
- De gegevensstroom van en naar SAP AIN/PAI naar de voorbeeldapplicatie.
    - Dit bevat de kraangegevens, de bedrijfsinformatie van de klant en contactgegevens van het onderhoudsteam.”



Figuur 5 SAP AIN

(SAP, IAM100 - SAP Intelligent Asset Management Overview , 2021)

Dus: Ja. De gegevensstroom van de NXT Brick naar de SAP omgeving bevat bedrijfsgegevens van het kraanbedrijf & de gegevensstroom van en naar SAP naar de voorbeeldapplicatie bevat kraangegevens, bedrijfsinformatie van de klant en contact/persoonsgegevens van de Business Partners. Een onderhoudsteam kan beschouwd worden als zo’n business Partner.

3. Verwerk ik deze gegevens geheel of gedeeltelijk geautomatiseerd, of zijn ze opgenomen in een bestand, dan wel bestemd om opgenomen te worden in een bestand?

De persoonsgegevens worden tijdens de Demo opgeslagen in het SAP platform. Verder is er geen bestand waar deze gegevens in zijn opgenomen. Wanneer de Demo wordt toegepast in de praktijk bij een klant, dan zal er in de meeste gevallen wel een bestand met klantgegevens zijn.

“SAP Asset Intelligence Network provides a virtual platform for collaboration on products and assets. The network of digital twins enables secure data access, sharing and governance on a global scale.”

Vertaling

“SAP Asset Intelligence Network biedt een virtueel platform voor samenwerking op het gebied van producten en activa. Het netwerk van digitale tweelingen maakt veilige datatoegang, -deling en -beheer op wereldwijde schaal.”

(SAP, IAM100 - SAP Intelligent Asset Management Overview , 2021)

Dus Atos voldoet met deze Demo Lego Kraan aan de AVG wetgeving. Verder focussen we ons dan op hoe zij hun klanten, waarbij deze demonstratie wordt geïmplementeerd, volgens deze wetgeving kunnen laten werken en waar ze daarbij aan moeten denken. We gaan er dan vanuit dat deze klanten persoonsgegevens hebben verwerkt in een bestand.

Wanneer u deze drie vragen met ‘ja’ heeft beantwoord moet u de volgende vraag beantwoorden:

4. Valt mijn verwerking binnen het toepassingsbereik van de Verordening?

“De Verordening geldt niet voor de hele wereld. Grofweg beperkt het territoriale bereik van de Verordening zich tot de volgende situaties:

• Organisaties (en personen) die in de Europese Unie gevestigd zijn en persoonsgegevens verwerken;

• Organisaties (en personen) die niét in de Europese Unie gevestigd zijn, maar wel gegevens verwerken van burgers in de EU”

(Bart W. Schermer, Dominique Hagenauw, Nathalie Falot, 2018)

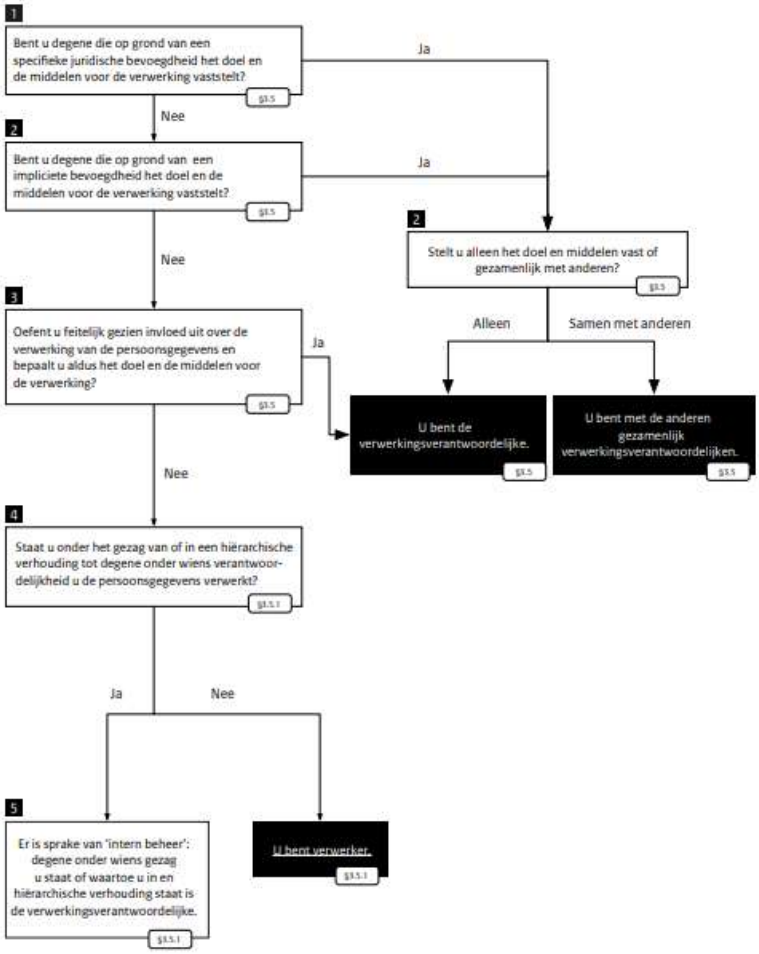
Dus: Ja. De verwerking van de gegevens passen binnen het toepassingsbereik van de verordening.

Als u deze vraag positief beantwoordt, dan is de Verordening op uw verwerking van toepassing. U moet dan alleen nog vaststellen wat uw juridische hoedanigheid is onder de Verordening, omdat deze bepaalt welke regels op u van toepassing zijn. Hiertoe stelt u zichzelf de volgende vraag:

5. Ben ik de verwerkingsverantwoordelijke, of ben ik een verwerker?

Schema 3: 1 -> 2 -> alleen -> U bent de verwerkingsverantwoordelijke (bij sommige klanten zou dit eventueel gezamenlijk met anderen kunnen zijn).

Schema 3: Bent u een verwerkingsverantwoordelijke of verwerker?

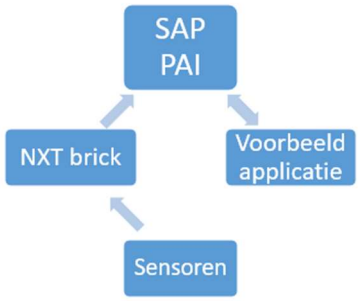


Figuur 6 Verwerkingsverantwoordelijkheid

BIJLAGE IV: DE AVG CHECKLIST

Figuur 7 AVG Checklist

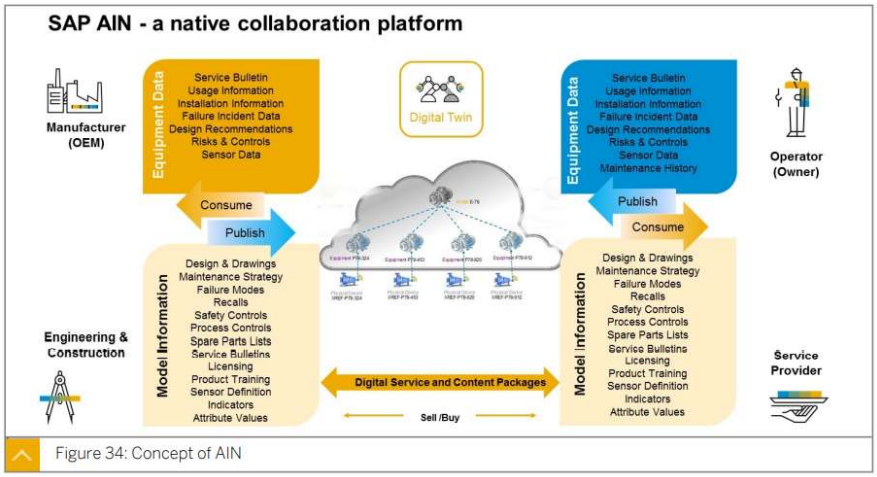
(Checklist, sd)



Figuur 8 Gegevensstroom

"De interfaces bestaan uit 3 gegevensstromen:

- Gebruiksgegevens van de sensoren naar de NXT Brick device;
    - De drukgegevens vanuit de sensor naar het ontvangende systeem gestuurd.
- De gegevensstroom van de NXT Brick naar de SAP AIN/PAI omgeving (de NXT Brick dient hierbij als gateway);
    - De druk- en bedrijfsgegevens worden vanuit het NXT Brick naar SAP AIN/PAI gestuurd. Dit bevat de gegevens over de kraan, het bedrijf dat de kraan gebruikt en wat de huidige sensor output is.
- De gegevensstroom van en naar SAP AIN/PAI naar de voorbeeldapplicatie.
    - Dit bevat de kraangegevens, de bedrijfsinformatie van de klant en contactgegevens van het onderhoudsteam."



Figuur 9 SAP AIN

(SAP, IAM100 - SAP Intelligent Asset Management Overview , 2021)

Dus: Ja. De gegevensstroom van de NXT Brick naar de SAP omgeving bevat bedrijfsgegevens van het kraanbedrijf & de gegevensstroom van en naar SAP naar de voorbeeldapplicatie bevat kraangegevens, bedrijfsinformatie van de klant en contact/persoonsgegevens van de Business Partners. Een onderhoudsteam kan beschouwd worden als zo'n business Partner.

ONDERDEEL C, D

De persoonsgegevens worden tijdens de Demo opgeslagen in het SAP platform. Verder is er geen bestand waar deze gegevens in zijn opgenomen. Wanneer de Demo wordt toegepast in de praktijk bij een klant, dan zal er in de meeste gevallen wel een bestand met klantgegevens zijn. Hierbij zullen alleen de gemachtigde toegang hebben tot dit onderdeel binnen het SAP platform en dit wordt gedaan door middel van restricties op de gebruikersaccounts.

“SAP Asset Intelligence Network provides a virtual platform for collaboration on products and assets. The network of digital twins enables secure data access, sharing and governance on a global scale.”

Vertaling

“SAP Asset Intelligence Network biedt een virtueel platform voor samenwerking op het gebied van producten en activa. Het netwerk van digitale tweelingen maakt veilige datatoegang, -deling en -beheer op wereldwijde schaal.”

(SAP, IAM100 - SAP Intelligent Asset Management Overview , 2021)

Dus Atos voldoet met deze Demo Lego Kraan aan de AVG wetgeving. Verder focussen we ons dan op hoe zij hun klanten, waarbij deze demonstratie wordt geïmplementeerd, volgens deze wetgeving kunnen laten werken en waar ze daarbij aan moeten denken. We gaan er dan vanuit dat deze klanten persoonsgegevens hebben verwerkt in een bestand.

ONDERDEEL E

Atos maakt gebruik van het SAP systeem en hierdoor worden de gegevens in het SAP systeem geplaatst. Met het aangaan van het contract voor het gebruik van dit systeem wordt beschreven dat Atos zelf verantwoordelijk is voor het plaatsen van de gegevens in het SAP systeem. SAP is daarin tegen verantwoordelijk voor alle gegevens die staan in haar systemen en daardoor ook verantwoordelijk voor de ingevoerde klantgegevens.

ONDERDEEL F

Atos heeft een Data Protection Officer aangesteld (PDO).

ONDERDEEL G, H

Dit is aanwezig, maar vanwege dat deze procedure intern is gesteld wordt deze niet beschreven.

BIJLAGE V: ISO27002 CHECK

INTELLECTUEEL EIGENDOM

Er moeten passende procedures worden ingevoerd om de naleving te waarborgen van wet- en regelgeving en contractuele vereisten in verband met intellectuele eigendomsrechten en het gebruik van prioritaire softwareproducten.

A. de publicatie van een beleid inzake de naleving van intellectuele-eigendomsrechten waarin het legale gebruik van software en informatieproducten;
B. het uitsluitend aanschaffen van software via bekende en gerenommeerde bronnen, om ervoor te zorgen dat het auteursrecht niet wordt geschonden
C. het op de hoogte houden van het beleid ter bescherming van intellectuele-eigendomsrechten en het bekendmaken van het voornemen om disciplinaire maatregelen te nemen tegen personeel dat deze rechten schendt
D. het bijhouden van passende activaregisters en het identificeren van alle activa die moeten voldoen aan de vereisten inzake de bescherming van intellectuele-eigendomsrechten;
E. Het bijhouden van bewijs van eigendom van licenties, master disks, handleidingen, enz.;
F. het uitvoeren van controles om ervoor te zorgen dat het binnen de licentie toegestane maximumaantal gebruikers niet wordt overschreden;
G. het uitvoeren van controles om ervoor te zorgen dat alleen geautoriseerde software en producten waarvoor een licentie is verleend, worden geïnstalleerd
H. het uitstippelen van een beleid om passende licentievoorwaarden te handhaven
I. het voorzien in een beleid voor het weggooien of overdragen van software aan anderen
J. het naleven van voorwaarden voor software en informatie verkregen van openbare netwerken
K. het niet verveelvoudigen, omzetten naar een ander formaat of uittreksels maken van commerciële opnamen (film, audio) anders dan toegestaan door de auteurswet;
L. het geheel of gedeeltelijk kopiëren van boeken, artikelen, rapporten of andere documenten, tenzij dit door de auteurswet is toegestaan.

Onderdeel	Check	Eventuele opmerking
A	Ja	Lego NXT heeft een gratis legale programmeer tool.
B	Ja	
C	N.v.t.	
D	N.v.t.	
E	Ja	Atos dient binnen SAP en Microsoft SharePoint de AVG/GDPR te handhaven.
F	Ja	Lego NXT heeft geen limiet qua maximaal aantal gebruikers.
G	Ja	Lego NXT heeft geen licentie nodig. De handhaving hierop is dus niet van belang.
H	N.v.t.	
I	N.v.t.	
J	Ja	Hierbij dient iedere medewerker te handelen naar eigen inzichten.
K	Ja	Doordat er geen licenties e.d. verbonden zijn aan de demo situatie zijn hier ook geen auteursrechten op. Indien dit door Atos wel gewenst is, dan zullen zij dit moeten verklaren.
L	N.v.t.	

Tabel 4 ISO27002 Intellectueel eigendom check

VERTROUWELIJKHEID

Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie voor van de organisatie voor de bescherming van informatie moeten worden vastgesteld, regelmatig herzien en gedocumenteerd.

A. een definitie van de te beschermen informatie (b.v. vertrouwelijke informatie)
B. de verwachte duur van een overeenkomst, met inbegrip van gevallen waarin vertrouwelijkheid eventueel voor onbepaalde tijd moet worden gehandhaafd;
C. vereiste acties wanneer een overeenkomst wordt beëindigd;
D. verantwoordelijkheden en acties van ondertekenaars om ongeoorloofde openbaarmaking van informatie te voorkomen;
E. eigendom van informatie, handelsgeheimen en intellectuele eigendom, en hoe dit zich verhoudt tot de bescherming van vertrouwelijke informatie;
F. het toegestane gebruik van vertrouwelijke informatie en de rechten van de ondertekenaar om informatie te gebruiken
G. het recht om audits uit te voeren en toezicht te houden op activiteiten waarbij vertrouwelijke informatie betrokken is
H. de procedure voor kennisgeving en rapportage van ongeoorloofde bekendmaking of het uitlekken van vertrouwelijke informatie
I. voorwaarden voor teruggave of vernietiging van informatie bij beëindiging van de overeenkomst
J. verwachte maatregelen die moeten worden genomen in geval van schending van de overeenkomst.

Onderdeel	Check	Eventuele opmerking
A	Ja	Alle gegevens dienen via de AVG behandeld te worden.
B	Ja	Wanneer een klant een overeenkomst met Atos aangaat dient dit gehanteerd te worden.
C	Ja	Alle gegevens dienen volgens de AVG verwerkt te worden of mogelijk verwijderd te worden.
D	Ja	De geheimhoudingsverklaring vanuit Atos dient gehanteerd te worden.
E	N.v.t.	
F	N.v.t.	
G	Ja	Alle gegevens dienen via de AVG behandeld te worden.
H	Ja	Wanneer er ongeoorloofde bekendmaking of uitlekken plaats vindt, dient de procedure van Meldplicht Datalek gehanteerd te worden. (Link)
I	Ja	Wanneer een overeenkomst wordt beëindigd dienen de gegevens volgens de AVG behandeld te worden. Hierbij mogen deze alleen opgeslagen blijven wanneer van de kraan waar geen klantgegevens aan gekoppeld zijn.
J	N.v.t.	

Tabel 5 ISO27002 vertrouwlijkheid check

BELEID

Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot informatie van de organisatie, deze verwerkt, opslaat of communiceert, of die IT-infrastructuurcomponenten levert voor de informatie van de organisatie.

A. beschrijving van de informatie die moet worden verstrekt of waartoe toegang moet worden verkregen en methoden voor het verstrekken van of de toegang tot de informatie;
B. classificatie van de informatie volgens het classificatiesysteem van de organisatie (zie 8.2); indien nodig ook het in kaart brengen van het eigen classificatiesysteem van de organisatie en het classificatiesysteem schema van de leverancier;
C. eisen op het gebied van wet- en regelgeving, met inbegrip van gegevensbescherming, intellectuele-eigendomsrechten en auteursrechten, en een beschrijving van de wijze waarop zal worden gewaarborgd dat hieraan wordt voldaan;
D. de verplichting van elke contract sluitende partij om een overeengekomen reeks controles uit te voeren, met inbegrip van toegangscontrole, prestatiebeoordeling, monitoring, rapportage en auditing;
E. regels voor het aanvaardbare gebruik van informatie, indien nodig met inbegrip van onaanvaardbaar gebruik
F. een expliciete lijst van leveranciers die toegang hebben tot informatie van de organisatie of deze mogen ontvangen of procedures of voorwaarden voor autorisatie, en verwijdering van de autorisatie, voor toegang tot of ontvangst van de informatie van de organisatie door personeel van de leverancier;
G. het informatiebeveiligingsbeleid dat relevant is voor het specifieke contract
H. eisen en procedures voor incidentenbeheer (met name kennisgeving en samenwerking tijdens het herstel van incidenten);
I. opleidings- en bewustmakingsvereisten voor specifieke procedures en informatiebeveiligingseisen, b.v. voor reactie op incidenten, autorisatieprocedures;
J. relevante voorschriften voor uitbesteding, met inbegrip van de controles die moeten worden uitgevoerd
K. relevante overeenkomstpartners, met inbegrip van een contactpersoon voor informatiebeveiligingskwesties
L. eventuele vereisten inzake het veiligheidsonderzoek van het personeel van de leverancier, met inbegrip van de verantwoordelijkheden voor het veiligheidsonderzoek en de kennisgevingsprocedures indien het veiligheidsonderzoek niet is voltooid of indien de resultaten aanleiding geven tot twijfel of bezorgdheid;
M. het recht om de processen en controles van de leverancier in verband met de overeenkomst aan een audit te onderwerpen
N. procedures voor het oplossen van gebreken en het oplossen van conflicten
O. de verplichting van de leverancier om periodiek een onafhankelijk verslag in te dienen over de doeltreffendheid van de controles en overeenkomst over tijdige correctie van relevante kwesties die in het verslag aan de orde worden gesteld;
P. de verplichtingen van de leverancier om te voldoen aan de beveiligingseisen van de organisatie.

Onderdeel	Check	Eventuele opmerking
A	Ja	Dit wordt gedaan door middel van een implementatieplan en adviesdocument.
B	N.v.t.	
C	Ja	Dit onderdeel verwijst naar de AVG.
D	N.v.t.	
E	N.v.t.	
F	N.v.t.	Dit wordt in het latere stadium geregeld door Atos in SAP.
G	Ja	
H	N.v.t.	
I	Ja	Het programmeren dient op een correcte werkwijze gedaan te worden door mensen met kennis over Lego NXT.
J	N.v.t.	
K	N.v.t.	De demo situatie bevat Lego onderdelen en in verdere stadium dient hier een contract met mogelijke partners te worden gesloten.
L	N.v.t.	
M	Ja	
N	Ja	Het lego onderdeel dient vervangen (geprogrammeerd) te worden door een exacte kopie hiervan.
O	Ja	
P	Ja	

Tabel 6 ISO27002 beleid check

AUDITING

Organisaties moeten de dienstverlening van leveranciers regelmatig controleren, evalueren en auditen.

A. de prestatieniveaus van de diensten te controleren om na te gaan of de overeenkomsten worden nageleefd
B. de door de leverancier opgestelde verslagen over de dienstverlening te beoordelen en regelmatig voortgangsvergaderingen te beleggen, zoals vereist zoals vereist in de overeenkomsten;
C. audits van leveranciers uit te voeren, in combinatie met een beoordeling van de verslagen van onafhankelijke auditors, indien beschikbaar en follow-up van de vastgestelde problemen;
D. informatie te verstrekken over incidenten op het gebied van informatiebeveiliging en deze informatie te beoordelen zoals vereist in de overeenkomsten en eventuele ondersteunende richtsnoeren en procedures
E. de audit trails en registers van de leverancier met betrekking tot informatiebeveiligingsincidenten, operationele problemen storingen, het traceren van fouten en verstoringen in verband met de geleverde dienst
F. vastgestelde problemen op te lossen en te beheren
G. de informatiebeveiligingsaspecten van de relaties van de leverancier met zijn eigen leveranciers te beoordelen
H. ervoor zorgen dat de leverancier over voldoende capaciteit voor dienstverlening blijft beschikken, samen met uitvoerbare plannen die ervoor moeten zorgen dat de overeengekomen continuïteitsniveaus worden gehandhaafd na belangrijke storingen of rampen.

Onderdeel	Check	Eventuele opmerking
A	N.v.t.	
B	N.v.t.	
C	Ja	
D	Ja	Wanneer een sensor een foutmelding of limiet heeft bereikt geeft deze een melding.
E	N.v.t.	
F	Ja	Atos dient onderhoudsmonteur in te schakelen.
G	N.v.t.	
H	N.v.t.	

Tabel 7 ISO27002 Auditing check

RAPPORTAGE

Gebeurtenissen op het gebied van informatiebeveiliging moeten zo snel mogelijk via de juiste managementkanalen worden gemeld.

A. ondoeltreffende beveiligingscontrole;
B. schending van de verwachtingen op het gebied van informatie-integriteit, vertrouwelijkheid of beschikbaarheid
C. menselijke fouten
D. niet-naleving van beleidslijnen of richtsnoeren
E. inbreuken op fysieke beveiligingsvoorzieningen
F. ongecontroleerde systeemwijzigingen
G. storingen in software of hardware
H. toegangsschendingen.

Onderdeel	Check	Eventuele opmerking
A	N.v.t.	
B	Ja	
C	Ja	
D	Ja	
E	N.v.t.	
F	Ja	
G	Ja	
H	Ja	

Tabel 8 ISO27002 Rapportage check