|  |
| --- |
| Adviesrapport Beveiligingsoplossing\_  Aan Impact IoT solutions |

Berkan Akdeniz, Tom Jager, Kaan Erköse

Hogeschool van Arnhem en Nijmegen

Minor Smart Industry

12 januari 2024

**MANAGEMENTSAMENVATTING**

In oktober 2023 is een projectgroep van de minor Smart Industry van de HAN gestart met een onderzoek voor het bedrijf Impact IOT Solutions. Hierbij is onderzocht wat juridische en organisatorische gevolgen zijn van een voorgestelde oplossing voor het beveiligingsprobleem bij Tautliners.

**Hoofdvraag en onderzoeksopzet**

De centrale vraag tijdens het onderzoek was als volgt: "Wat zijn de juridische en organisatorische gevolgen van de voorgestelde oplossing voor het tautliner-beveiligingsprobleem?"

Om deze vraag te beantwoorden is er onderzoek gedaan naar de achtergrond van het vraagstuk en zijn vier deelvragen beantwoord. Deze deelvragen waren als volgt:

1. Wat zijn de juridische consequenties van het implementeren van camera's, data en AI voor vrachtbeveiliging?
2. Zijn er aanpassingen aan de huidige wetgeving nodig om deze nieuwe technologieën te integreren?
3. Wat is de impact van de voorgestelde oplossing op organisaties in de betrokken sectoren?
4. Zullen bestaande werkmethoden moeten worden aangepast om de nieuwe beveiligingsoplossing te kunnen gebruiken?

**Belangrijke resultaten**

Op juridisch gebied is de belangrijkste uitkomst een tabel met wetten voor én tegen de oplossing geweest. Deze tabel is terug te vinden in de bijlage van dit document.   
Op organisatorisch gebied is het verschil tussen de huidige situatie en toekomstige situatie erg belangrijk geweest.

**Advies**

Als advies aan Impact IOT Solutions kan de volgende samenvatting gegeven worden. Voor implementatie van de beveiligingsoplossing is het noodzakelijk om te voldoen aan de beginselen van de AVG. Hierbij zijn de belangrijkste principes: rechtmatigheid, doelbinding, dataminimalisatie, transparantie en duidelijkheid. Een DPIA kan toevoeging bieden om aan dit vereiste aan te pakken. Verder is het aan te raden om douane- en logistiek personeel voor te bereiden op veranderingen in hun werkzaamheden. Dit kan gedaan worden door het geven van trainingen. Daarnaast is het verstandig om de gehele keten bij de implementatie van de technologische oplossing te betrekken. Dit zorgt voor afstemming en duidelijkheid bij elke belanghebbende in de organisaties. Als laatste is het belangrijk om vroegtijdig het exterieur van Tautliners aan te passen.

INHOUDSOPGAVE

[INLEIDING 4](#_Toc155985686)

[1 onderzoek 5](#_Toc155985687)

[2 Advies 6](#_Toc155985688)

[2.1 Juridisch Advies 6](#_Toc155985689)

[2.2 Organisatorisch Advies 6](#_Toc155985690)

[2.3 Data Protection Impact Assessment (DPIA) 7](#_Toc155985691)

[3 conclusie 9](#_Toc155985692)

[bronnenlijst 10](#_Toc155985693)

[bijlagen 11](#_Toc155985694)

[Bijlage 1: artikelen voor én tegen de oplossing 11](#_Toc155985695)

INLEIDING

In oktober 2023 is een projectgroep van de minor Smart Industry van de HAN gestart met een onderzoek voor het bedrijf Impact IOT Solutions. Dit technologiebedrijf is gevestigd in Doetinchem en is gespecialiseerd in het ontwikkelen van innovatieve IOT-oplossingen.

Het onderzoek ging over internationaal wegtransport van Tautliners tussen Nederland en het Verenigd Koninkrijk. Een Tautliner is een trailer dat voorzien is van een zeil aan de zijkanten ervan. In verband met dit zeil wordt er met regelmaat gesjoemeld met de lading. Om dit tegen te gaan wordt de Tautliner verzegeld met koord, opzetstuk en loodje. Het aanbrengen van het zegel kost behoorlijk veel tijd en duurt ca. 30 minuten. Daarnaast gebeuren er nog steeds vaak verdachte activiteiten. Hierdoor is er een oplossing bedacht om in de toekomst de Tautliner met een technologische innovatie te beveiligen. Hierbij wordt de trailer gemonitord met een camera, data en kunstmatige intelligentie.

Concreet hebben wij onderzoek gedaan naar de juridische en organisatorische gevolgen van deze technologische innovatie. Hierbij was onze doelstelling om een adviesrapport te schrijven aan Pieter Hoenderken, directeur van Impact IOT Solutions. Deze doelstelling is verwoord in de volgende hoofdvraag:

"Wat zijn de juridische en organisatorische gevolgen van de voorgestelde oplossing voor het Tautliner- beveiligingsprobleem?"

In het eerste hoofdstuk is informatie te lezen over de stappen in het onderzoek. Het tweede hoofdstuk bestaat uit het juridische en organisatorische advies op basis van de oplossing. In het derde hoofdstuk wordt een conclusie van dit uitgebreide advies geschreven.

# onderzoek

Bij het onderzoek zijn vijf stappen doorlopen. De eerste stap was het onderzoeken van de achtergrond van het project. De overige vier stappen bestonden uit deelvragen, die de volgende waren:

1. Wat zijn de juridische consequenties van het implementeren van camera's, data en AI voor vrachtbeveiliging?
2. Zijn er aanpassingen aan de huidige wetgeving nodig om deze nieuwe technologieën te integreren?
3. Wat is de impact van de voorgestelde oplossing op organisaties in de betrokken sectoren?
4. Zullen bestaande werkmethoden moeten worden aangepast om de nieuwe beveiligingsoplossing te kunnen gebruiken?

De belangrijkste uitkomst van het juridische gedeelte van het onderzoek is een tabel geworden met wetten die voor én tegen de oplossing zijn. Deze tabel is in de bijlage opgenomen.

De belangrijkste uitkomst van het organisatorische gedeelte van het onderzoek zijn de inzichten geweest in het verschil tussen huidige en toekomstige situatie.

Op basis van deze uitkomsten is het advies geformuleerd.

# Advies

Op basis van het onderzoek omtrent de juridische en organisatorische gevolgen van de voorgestelde oplossing voor het Tautliner-beveiligingsprobleem, stellen wij de volgende aanbevelingen voor in het adviesrapport:

## Juridisch Advies

**2.1.1 Naleving van de Algemene Verordening Gegevensbescherming (AVG):**

* Zorg ervoor dat alle aspecten van het gebruik van camera's, data, en kunstmatige intelligentie (AI) voldoen aan de beginselen van de AVG.
* Houd rekening met principes zoals rechtmatigheid, doelbinding, dataminimalisatie, transparantie, en implementeer passende beveiligingsmaatregelen.
* Zorg ervoor dat overeenkomsten zijn getekend met belanghebbenden om rechtvaardig te werken (zie hoofdstuk 2.3 als voorbeeld van een overeenkomst).

**2.1.2 Duidelijkheid en transparantie**

* Communiceer duidelijk met betrokkenen over het doel van gegevensverzameling en -verwerking.
* Zorg voor transparantie in het gebruik van AI en wees helder over de wettelijke basis en toestemming.

**2.1.3 Overige wetten**

* Neem andere relevante wetten, zoals de Wet politiegegevens, Telecommunicatiewet, EVRM, en de Wet op de inlichtingen- en veiligheidsdiensten, op in uw juridisch kader.
* Besteed bijzondere aandacht aan situaties gerelateerd aan veiligheid en surveillance.

## Organisatorisch Advies

**2.2.1 Aanpassingen in douanecontroles**

* Bereid douanepersoneel voor op de overgang naar gerichte controles op basis van verdachte beelden.
* Implementeer training om douanepersoneel vertrouwd te maken met de nieuwe technologische benaderingen.

**2.2.2 Investeringen voor transportbedrijven**

* Erken de initiële investeringskosten voor transportbedrijven en benadruk de lange termijnvoordelen van verbeterde operationele efficiëntie.
* Faciliteer trainingssessies voor personeel om hen voor te bereiden op nieuwe procedures.

**2.2.3 Overreding van software- en hardwareleveranciers**

* Ontwikkel overtuigende argumenten en voordelen om software- en hardwareleveranciers te betrekken bij de implementatie.
* Onderhandel over samenwerking om de technologische oplossing succesvol te integreren.

**2.2.4 Betrokkenheid van verzekeraars**

* Informeer verzekeraars over de voordelen van de voorgestelde beveiligingsmaatregelen en hun impact op risicobeoordelingen.
* Werk samen om mogelijkheden te verkennen voor aanpassingen van verzekeringspremies.

**2.2.5 Operationele aanpassingen**

* Anticipeer op potentiële aanpassingen in logistieke processen als gevolg van de nieuwe controlemechanismen.
* Faciliteer training en bewustwordingsprogramma's om een soepele overgang te waarborgen.

## Data Protection Impact Assessment (DPIA)

Een essentieel onderdeel van het advies met betrekking tot de voorgestelde oplossing voor het Tautliner-beveiligingsprobleem is de implementatie van een Data Protection Impact Assessment (DPIA). Dit proces biedt een gestructureerde methode om de potentiële gevolgen van gegevensverwerking op de privacy en gegevensbescherming te beoordelen. Hier zijn enkele richtlijnen met betrekking tot DPIA:

**2.3.1 Vroegtijdige DPIA-uitvoering**

* Voer de DPIA vroeg in het ontwikkelingsproces uit om eventuele privacyrisico's en nalevingskwesties in een vroeg stadium te identificeren en aan te pakken.

**2.3.2 Betrokkenheid stakeholders**

* Betrek relevante belanghebbenden, inclusief juridische experts, IT-specialisten, en vertegenwoordigers van privacyrechtenorganisaties, om een uitgebreid begrip van de mogelijke impact te waarborgen.

**2.3.3 Naleving van AVG-principes**

* Zorg ervoor dat de DPIA volledig voldoet aan de principes van de Algemene Verordening Gegevensbescherming (AVG).
* Richt de beoordeling op specifieke aspecten zoals gegevensverzameling, doelbinding, dataminimalisatie, en beveiligingsmaatregelen.

**2.3.4 Risicobeoordeling**

* Identificeer potentiële risico's voor de privacy en gegevensbescherming en formuleer maatregelen om deze risico's te verminderen of te elimineren.
* Documenteer zorgvuldig alle risico's en genomen maatregelen.

**2.3.5 Transparantie en communicatie**

* Communiceer helder over de DPIA-resultaten naar alle betrokkenen, inclusief werknemers, klanten en andere relevante partijen.
* Benadruk de genomen maatregelen om privacy en gegevensbescherming te waarborgen.

**2.3.6 Continue evaluatie**

* Implementeer een proces voor voortdurende evaluatie en herbeoordeling van de DPIA in overeenstemming met de evoluerende technologieën en veranderende wet- en regelgeving.

**2.3.7 Betrekking op juridische en organisatorische aspecten**

* Integreer de DPIA in zowel juridische als organisatorische overwegingen, waarbij aandacht wordt besteed aan de impact op de bedrijfsprocessen en het juridisch kader.

Door het opnemen van een grondige DPIA in het implementatieproces van de voorgestelde beveiligingsoplossing, zal de organisatie niet alleen voldoen aan wettelijke vereisten, maar ook proactief privacyrisico's aanpakken en het vertrouwen van belanghebbenden versterken. De DPIA dient als een waardevol instrument om een evenwicht te vinden tussen innovatie en gegevensbescherming voor van het Tautliner-beveiligingsprobleem.

# conclusie

Het adviesrapport benadrukt de cruciale aspecten van de voorgestelde oplossing voor het Tautliner-beveiligingsprobleem, met een focus op zowel juridische als organisatorische overwegingen.

Op juridisch gebied blijkt de Algemene Verordening Gegevensbescherming (AVG) van centraal belang te zijn, en het naleven van de beginselen ervan is essentieel om gegevensbescherming en privacy te waarborgen bij het gebruik van camera's, data en kunstmatige intelligentie (AI). Hierbij kan een DPIA het juridische gedeelte versterken.

Het organisatorische advies richt zich op het anticiperen op de impact van de voorgestelde beveiligingsoplossing op verschillende sectoren, met specifieke aandacht voor douanecontroles, investeringen voor transportbedrijven, overreding van software- en hardwareleveranciers, betrokkenheid van verzekeraars en operationele aanpassingen. Het is duidelijk dat een gebalanceerde benadering nodig is, waarbij de initiële uitdagingen worden omgezet in lange termijnvoordelen.

bronnenlijst

Al-Safi, H., Tanribuyurdu, O., Planjer, B., Özmen, E., & Metzen, R. (2023). Kan objectdetectie van YOLO, in achtneming van de probleemstelling van de Douane, met behulp van camera’s worden toegepast? [Ongepubliceerde praktijkopdracht]. Hogeschool Windesheim.

Busby, A., Lievestro, J., & Van Schip, Y. (z.d.). Het bedenken van een slimme innovatieve verzegeling voor zeiltrailers [Ongepubliceerd onderzoek]. Ulenhof College.

Consultancy.nl. (2021, 21 juni). Optimaliseer de fysieke beveiliging in de logistieke sector. Consultancy. Geraadpleegd op 1 november 2023, van <https://www.consultancy.nl/nieuws/35262/optimaliseer-de-fysieke-beveiliging-in-de-logistieke-sector>

De Ruijt, C. (2023). Engineering a digital seal for Tautliner transport to/from the UK [Ongepubliceerde memo]. Hogeschool Windesheim.

Hutter, J. (2016, 21 september). Meldplicht datalekken. Inview Essential. <https://www.inview.nl/thema/idpass254beb2cea9b46ca957e110253607fbf/meldplicht-datalekken?anchor=auteur&referrer=classic-navigator>

J.Oerlemans & A. Drahmann (9-11-2023) Publiekrecht en digitalisering. <https://www.inview.nl/document/idc281a0758bc64f8eaedab845ebdc925c/computerrecht-publiekrecht-en-digitalisering?ctx=WKNL_CSL_26&tab=tekst>

Networking4all B.V. (z.d.). Cybersecurity in de transport | MSSP. Networking4all Cybersecurity Specialist. <https://www.networking4all.com/nl/security/branches/transport>

Regels Cameratoezicht voor organisaties. (z.d.). Autoriteit Persoonsgegevens. <https://www.autoriteitpersoonsgegevens.nl/themas/cameratoezicht/cameratoezicht-bij-organisaties/regels-cameratoezicht-voor-organisaties>.

Talia, M. (2022, 20 juli). Ways to keep fleet vehicles running Efficiently | Linxio. Linxio. <https://linxio.com/gps-tracking-benefits-in-transport-industry/>

TAPA - Kenniscentrum Veiligheid365. (2021, 29 januari). Kenniscentrum Veiligheid365. <https://www.veiligheid365.nl/certificeringen/tapa/>

Van der Jagt, F. (2023, 9 augustus). Algemene Verordening Gegevensbescherming (AVG). Inview Essential. <https://www.inview.nl/thema/idpass7a2fc735e3d7438195700b537eee4dab/algemene-verordening-gegevensbescherming-avg?anchor=auteur>

bijlagen

## Bijlage 1: artikelen voor én tegen de oplossing

|  |  |
| --- | --- |
| Artikelen voor | Artikelen tegen |
| Het identificeren van een wettelijke grondslag voor de verwerking van persoonsgegevens, zoals bepaald in Artikel 6 AVG, is ook cruciaal. Mogelijke grondslagen kunnen onder andere toestemming van betrokkenen, **uitvoering van een overeenkomst** (DPIA), **wettelijke verplichtingen**, **bescherming van vitale belangen**, **vervulling van een taak van algemeen belang**, of **de uitoefening van openbaar gezag zijn.** | Om ervoor te zorgen dat **betrokkenen** hun rechten kunnen uitoefenen, waaronder **het recht op inzage, rectificatie, wissing van gegevens, beperking van verwerking, bezwaar tegen verwerking en gegevensoverdraagbaarheid (Artikel 15-22 AVG), is transparantie en toegankelijkheid van informatie essentieel.** |
| De informatieplicht (Artikel 13 en 14 AVG) vereist dat **betrokkenen** **worden geïnformeerd over het gebruik van de camera's, inclusief het doel, de wettelijke basis voor verwerking, de bewaartermijn van gegevens en hun rechten.** | **Er zijn wel een aantal uitzonderingen waarbij de AVG niet in kracht is dat is namelijk:**   * **In het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen.** * **Door de lidstaten bij de uitvoering van grenscontroles, asiel en immigratie (Titel V, Hoofdstuk 2, VEU)** * **Door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van strafrechtelijke sancties, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.** * **Door de instellingen, organen en instanties van de Europese Unie** |
| **Persoonsgegevens moeten rechtmatig, behoorlijk en transparant worden verwerkt.** | **Dataminimalisatie (niet meer persoonsgegevens verwerken dan noodzakelijk is om de doeleinden te bereiken).** |
| **Door de lidstaten bij de uitvoering van grenscontroles, asiel en immigratie (Titel V, Hoofdstuk 2, VEU)** | **Persoonsgegevens mogen niet langer in een tot een individu te herleiden vorm worden bewaard dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt (opslagbeperking).** |
| **Persoonsgegevens mogen alleen worden verwerkt voor de doeleinden waarvoor ze verzameld zijn waarbij de welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden van tevoren zijn bepaald (zie ook artikel 6 lid 4 AVG), het zgn. doelbindingsbeginsel.** | **Persoonsgegevens moeten goed worden beveiligd (integriteit en vertrouwelijkheid waarborgen).** |
| **De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.** | De betrokkene heeft **toestemming** gegeven voor de verwerking van zijn of haar persoonsgegevens voor een of meerdere specifieke doeleinden. **Het is lastig om toestemming te vragen om gegevens te verwerken van een persoon die criminele activiteiten vertoond bij de trailers.** |
| **De juistheid van persoonsgegevens moet worden gewaarborgd, onder meer door deze te actualiseren indien nodig.** | **Expliciet is opgenomen dat overheidsinstanties geen beroep kunnen doen op de grondslag van het ‘gerechtvaardigdheid belang’ in het kader van de uitoefening van hun taken. Daarnaast worden strenge voorwaarden gestel aan gegevensverwerkingen die op toestemming zijn gebaseerd** |
| De verwerking is noodzakelijk ter uitvoering van een **overeenkomst** waarbij de betrokkene partij van is, of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen. **Een DPIA is een voorbeeld van zo’n overeenkomst** | Wanneer de verwerking berust op toestemming, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens. |
| De verwerking is **noodzakelijk om te voldoen aan een wettelijke verplichting** die op de verwerkingsverantwoordelijke rust. | Indien de betrokkene toestemming geeft in het kader van een **schriftelijke verklaring** die ook op andere aangelegenheden betrekking heeft, wordt het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. Wanneer een gedeelte van een dergelijke verklaring een inbreuk vormt op deze verordening, is dit gedeelte niet bindend. |
| De verwerking is **noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen**. | Bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, wordt onder meer ten sterkste rekening gehouden met de vraag of voor de uitvoering van een overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van die overeenkomst. De AVG stelt speciale eisen ten aan zien van het verkrijgen van toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij. In Nederland geldt dat een minderjarige minimaal 16 jaar oud moet zijn om geldige toestemming te kunnen verlenen. |
| De verwerking is **noodzakelijk voor het vervullen van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag** dat aan de verwerking verantwoordelijke is opgedragen. | Bepaalde categorieën van persoonsgegevens mogen niet verwerkt worden. Het gaat dan om **persoonsgegevens waarvan de verwerking significante risico’s kan meebrengen, voorbeelden hiervan zijn discriminatie of uitsluiting.** Dit zijn risico’s waarbij grondrecht en of fundamentele vrijheden van betrokkenen worden geschonden. |
| Artikel 35: Voordat je met AI begint, voer een DPIA uit als er een risico is voor de rechten en vrijheden van mensen. Het helpt om vooraf te begrijpen welke risico's je neemt en hoe je ze kunt verminderen. | Artikel negen van de AVG geldt dat verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden |
|  | Artikel 5:Als je AI gebruikt, moet je heel duidelijk zijn over **waarom je bepaalde gegevens verzamelt. Zorg dat het doel helder, specifiek en legitiem is**. Dit betekent dat je de data alleen voor bepaalde, vooraf bepaalde doeleinden mag gebruiken. |

