2021

IT-Audit

IT-WORKZ

SANDER VLUG, GEOFFREY HOSE, TIM GHIJSEN

Inhoudsopgave

1 Inleiding

1.1 Opdrachtomschrijving

1.1.1 Inleiding

Deze audit wordt uitgevoerd voor IT-Workz. IT-Workz is een ICT-bedrijf die zich focust op onderwijs en werkt veel samen met scholen. Deze scholen hebben aangegeven dat ze veel data hebben en hier vrij weinig mee doen.

De scholen vinden het belangrijk dat er op een innovatieve manier bedacht wordt hoe deze data gebruikt kan worden. Dit kan bijvoorbeeld door middel van voorspellingen. Voorspellingen kunnen gemaakt worden door Artificial Intelligence en Machine Learning in te schakelen. Hier heeft IT-Workz een idee en concept voor gemaakt. Het concept is de app Operationeel Medewerker Assistent (OMA). OMA zal de data van de scholen gaan gebruiken om hier verzuim van docenten te voorspellen. Het doel van het project is om een blauwdruk voor de applicatie OMA te maken. De blauwdruk is het grondwerk voor OMA. In de blauwdruk worden de waarden die uit de app OMA te halen zijn, de AVG en de wetgeging rond de benodigde data duidelijk beschreven. De blauwdruk wordt aan de scholen gegeven om hiermee de meeste vragen te kunnen beantwoorden. Het maken van de blauwdruk is deel van fase 0 van de OMA app. Hierin zal vooral aandacht besteed worden aan het begrijpen van het concept van de app, de behoefte van de scholen (klanten) en van de wetgeving rondom het uitbrengen van een app waar met persoonlijke gegevens gewerkt moet worden.

1.1.2 Aanleiding

De aanleiding van deze audit is, dat de klanten van IT-Workz gevraagd hebben om voorspellingen te doen met de data die beschikbaar is binnen de scholen. Hiervoor is het concept OMA ontstaan. De aanleiding van de audit is dat er goed naar de data gekeken moet worden en dat er aandacht besteed moet worden aan de AVG gerelateerde risico's die kunnen ontstaan tijdens het creëren en implementeren van de app. Om de OMA app zo effectief mogelijk te gebruiken moet er ook gekeken naar welke data gebruikt kan worden om het gewenste resultaat te krijgen.

Door een audit uit te voeren op de data die gebruikt mag worden zal IT-Workz een bevestiging krijgen of ze überhaupt de OMA app kunnen bouwen. Een van de grootste risico’s die deze IT-audit met zich meebrengt is dat met een negatief resultaat het hele project gestopt zal moeten worden. In andere woorden als de data niet gebruikt mag worden heeft dit een grote impact op het bouwen van de OMA app. Hierdoor is het belangrijk dat de IT-Audit in de beginfase van het project uitgevoerd wordt. Ondanks het risico dat de audit veel negatieve gevolgen heeft voor het project, zal het oordeel over de audit niet worden beïnvloed.

Om de OMA app functioneel te krijgen zullen er verschillende gevoelige data gebruikt worden, daarom is het belangrijk dat de data op een veilige manier verzameld en opgeslagen kan worden. De impact die een data lek kan hebben is erg hoog, daarom is het belangrijk dat alleen de juiste personen de juiste data kunnen inzien.

1.2 Normenkader en scope

1.2.1 Normenkader

Voor deze audit is er gekozen voor het PCF van NOREA. Dat komt omdat de NOREA een internationaal erkende audittors organisatie is met veel kennis. Daarbij sluit het PCF nauw aan op de 13 kernelementen van de AVG. Het PCF heeft verder een goede overlap met de NEN-ISO/IEC ISO 27001 en 27002 normenkaders. (de Heer, J. 2019, 1 augustus)

“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.” (NOREA - de beroepsorganisatie van IT-Auditors. z.d.)

Voor meer informatie over het PCF wordt u aangeraden om de officiële handleiding van het PCF te bekijken. Daar worden alle aspecten van het PCF tot in detail uitgelegd.

1.2.2 Scope

Tijdens de audit zal er exclusief naar de AVG-wetgeving gekeken worden. Dit gaat over welke persoonsgevoelige data er gebruikt kan worden in de app, hoe de data opgeslagen wordt en welke data opgeslagen mag worden. Er zal aandacht gegeven worden aan de veiligheid van de data en de compliance van de wetgeving. In het vooronderzoek is er een AVG-raamwerk uitgekozen die het meest past bij de OMA app. Dit raamwerk betreft het PCF framework.

Tijdens de audit zal er gekeken worden naar de data van de school SOML aangezien deze school als eerste interesse heeft getoond in het project OMA. Er is ondertussen overleg met andere scholen die wellicht aan willen sluiten, maar in de audit zal er dus beperkt worden tot SOML.

Verder wordt de audit beperkt door het project waar het aan verbonden is. Zo zal de audit niet verder gaan dan de blauwdrukken die eind juni zijn opgeleverd. Tijdens het maken van de app zal er een Data protection impact assessment (DPIA) moeten plaatsvinden. Deze DPIA zal niet in dit onderzoek komen, maar het onderzoek zal grondwerk zijn voor de DPIA.

1.3 Bijzonderheden opdracht

1.3.1 Ontwikkeling in vakgebied

De app OMA zal gebruik maken van Machine learning (ML). Hieronder staat de definitie van machine learning en artificial intelligence door IBM.

1.3.2 Wat is machine learning

Machine learning is een tak van kunstmatig intelligentie (AI) die zich toelegt op het bouwen van toepassingen die van gegevens leren en hun nauwkeurigheid in de loop van de tijd verbeteren zonder daartoe geprogrammeerd te zijn. (Education, I. C. 2021, 25 maart)

In data science is een algoritme een opeenvolging van statistische verwerkingsstappen. Bij machine learning worden algoritmen "getraind" om patronen en kenmerken te vinden in enorme hoeveelheden gegevens om op basis van nieuwe gegevens beslissingen en voorspellingen te doen. Hoe beter het algoritme, hoe nauwkeuriger de beslissingen en voorspellingen zullen worden naarmate het meer gegevens verwerkt.

1.3.3 Wat is AI

In de informatica verwijst de term kunstmatige intelligentie (AI) naar elke mensachtige intelligentie die wordt vertoond door een computer, robot of andere machine. In de volksmond verwijst kunstmatige intelligentie naar het vermogen van een computer of machine om de mogelijkheden van de menselijke geest na te bootsen - leren uit voorbeelden en ervaring, voorwerpen herkennen, taal begrijpen en erop reageren, beslissingen nemen, problemen oplossen - en deze en andere mogelijkheden te combineren om functies uit te voeren die een mens zou kunnen uitvoeren, zoals een hotelgast begroeten of een auto besturen. (Education, I. C. 2021b, 7 april)

De app OMA gaat gebruik maken van twee verschillende vormen van ML. Dit is supervised learning en deep learning. Hiervoor gaat (historische) data nodig zijn.

1.4 Ontwikkeling binnen de organisatie

De app zal gebruikt gaan worden door verschillende VO/MBO scholen in Nederland. Deze scholen zijn klanten van IT-Workz. Er zal samengewerkt worden met een school die als pilot de app gaat runnen. Hierdoor zal er geen ontwikkeling binnen de organisatie van IT-Workz plaatvinden maar wel in externe organisaties. Daar zal de app OMA de ontwikkeling zijn die verzuim voorspelt en acties zal aanbevelen voor de scholen om op te volgen.

1.5 Onderzoeksvragen

Voor de uitvoer van de audit zijn er onderzoeksvragen opgesteld. Dit is gedaan om ervoor te zorgen dat elk vlak goed onderzocht wordt. Deze hoofd- en deelvragen zijn goedgekeurd door de opdrachtgever en andere experts van IT-Workz. Dit is gedaan om de kwaliteit van de audit te waarborgen.

1. Welke data is noodzakelijk om de machine learning achter OMA voorspellingen te laten doen?
2. Welke data mag er verzameld en gebruikt worden volgens het passende AVG-raamwerk?
3. Hoe kan IT-Workz ervoor zorgen dat de data veilig opgeslagen wordt?

Deze audit werkt de deelvragen op volgorde uit. Dit is van belang omdat de mogelijke data variabelen (deelvraag 1) een afbakening vormen voor deelvraag 2. Er hoeft dan minder data getoetst te worden met het AVG-raamwerk. Deelvraag 2 vormt wederom een afbakening voor deelvraag 3, aangezien deelvraag 3 richtlijnen aanhaalt voor hoe de specifieke veilig opgeslagen kan worden.

2 Managementsamenvatting

2.1 Bevindingen, conclusies en advies

2.1.1 Deelvraag 1

2.1.1.1 Bevindingen

Deelvraag 1 luidt: *Welke data is noodzakelijk om de machine learning achter OMA voorspellingen te laten doen?*

In onderstaande tabel zijn alle bevindingen samengevat en uitgelegd. Hierbij is een “datapunt” een aparte soort data die de werking van OMA bevordert.

ID	Soort datapunt	Toelichting
1	Gegevens over medische klachten die al spelen. (Medische dossier)	Als OMA weet welke klachten docenten al hebben is het eenvoudiger om gepaste voorspellingen te doen.
2	Persoonsgegevens • Naam • Geslacht • Leeftijd • Woonplaats	De meest generieke persoonsgegevens vormen het basisprofiel van de gebruikers van OMA.
3	Verzuim meldingen; • Persoon • Datum/tijd • Duur • Klachten	Gegevens over verzuim dat plaats heeft gevonden.
4	Leeftijdsgebonden data	Hoeveel kans op ziekte X heb je als je Y jaar oud bent? Dit zijn externe openbare gegevens.
5	Conflicten met collega’s en leerlingen	De sfeer op school kan veel invloed hebben op de gezondheid van docenten.
6	Data per klas: • Verhouding man/vrouw • Niveau • Grootte • Blijven-hangers • Straffen	De sfeer op school kan veel invloed hebben op de gezondheid van docenten. Gegevens over de klas kunnen iets zeggen over de sfeer die er heerst.
7	Overwerken/roostergegevens: uren te veel • Controles met planningen • Tijd besteed aan voorbereidingen • Tijd besteed aan lesgeven • Tijd besteed aan nakijken • Teamsamenstelling	Gedetailleerde gegevens over de tijdsbesteding zeggen veel over stress die de docent ervaart.
8	Contract gegevens • Aantal dienstjaren • Omvang contract • Functie • Salaris groei • Opleiding • Koppeling persoonsgegevens	Specifieke gegevens over het contract zeggen veel over de stress die de docent ervaart.

9	Seizoensgebonden data	Statistieken over in welke periode mensen meer kans hebben om bepaalde ziektes op te lopen.
10	Landelijke trends	Sommige trends kunnen invloed hebben op het imuunsysteem. Ziektes zelf kunnen ook een trend zijn.
11	Vaccinaties	Voor welke ziektes is de docent gevaccineerd?
12	Thuissituatie • Getrouwd/alleenstaand • Kinderen	De thuissituatie kan iets zeggen over de stress die de docent ervaart.

Tabel 1: Datapunten met uitleg over waarom ze nuttig kunnen zijn voor de OMA app.

2.1.1.2 Advies

Alle datapunten in Tabel 1 zijn bevorderlijk voor de werking van de OMA app. Datapunt 2 vormt de basis; dit zijn de persoonsgegevens waar alle voorspellingen en adviezen aan gekoppeld worden. Verder zou OMA al goed uit de voeten kunnen met 1, 4, 7 en 8. Of deze datapunten ook daadwerkelijk gebruikt mogen worden hangt af van de resultaten van deelvraag 2.

2.1.2 Deelvraag 2

Deelvraag 2 luidt: *Welke data mag er verzameld en gebruikt worden volgens het passende AVG-raamwerk?*

Om te kijken welke variabelen uit tabel 1 gebruikt mogen worden, zal er eerst gekeken moeten worden welke variabelen bij de ‘’gewone’’ persoonsgegevens of de ‘’bijzondere’’ persoonsgegevens horen. De variabelen “gegevens over medische klachten” en “het vaccinatiepaspoort” vallen onder de bijzondere persoonsgegevens. Onder de gegevens van de klas kunnen persoonsgegevens van kinderen omvatten. De rest van de gegevens zijn ‘’gewone’’ persoonsgegevens. Deze verdeling van het onderscheid moet worden gecontroleerd en geconformeerd en gedocumenteerd worden door de uitbrengende partij van de app. Hiervoor zal een procedure opgesteld moeten worden. Voor “data per klas” wordt er geadviseerd om de gegevens te anonimiseren en ervoor te zorgen dat de gegevens niet terug te herleiden zijn naar personen/kinderen. Bij de persoonsgegevens van kinderen is er namelijk expliciet toestemming van de ouders nodig.

Bijzondere persoonsgegevens:

Voor de bijzondere persoonsgegevens wordt er in het PCF beschreven dat er uitdrukkelijke toestemming van de betrokkene nodig is. Dit betekent dat de personen waarvan de gegevens zijn in een formulier of vragenlijst toestemming moet geven door middel van een vakje aan te vinken. Dit moet gedocumenteerd en opgeslagen worden. Deze toestemming moet ook ten aller tijde ingetrokken kunnen worden door de betrokkenen. Er worden maatregelen getroffen om veilige verwerking volgens de geldende voorschriften te waarborgen door de uitbrengende partij van de app. Verder moeten de gegevens noodzakelijk zijn voor de werking van de app. Dit betekent in het geval van de medische gegevens, dat er eerst geprobeerd moet worden of de voorspellingen accuraat zijn zonder de medische gegevens. Indien de voorspellingen niet accuraat zijn kunnen de medische gegevens toegevoegd worden.

‘’Gewone’’ persoonsgegevens:

Het gebruik van de ‘’gewone” persoonsgegevens is mogelijk als de partij die de app uitbrengt (entiteit) voldoet aan de punten die op zijn gesteld in het privacy control framework (PCF) van NOREA. Voor het gebruik van de data wordt er geadviseerd dat de entiteit aan alle beheersingsdoelstellingen van het PCF voldoet. Hieronder vindt u een samenvatting van de belangrijkste beheersingsdoelstellingen in het PCF. Bij elke beheersingsdoelstelling hoort ook één of meerdere beheersingsmaatregelen. De volledige lijst van doelstellingen en maatregels die binnen het framework hoort kunt u vinden in de appendix in hoofdstuk 4 van dit document.

- De entiteit moet een privacy beleid opstellen.
- Er moeten duidelijke rollen en verantwoordelijkheden met betrekking tot bescherming van persoonsgegevens zijn.
- Er moet duidelijk gedocumenteerd worden welke gegevens opgeslagen worden.
- Er moet een risico analyse worden gemaakt.
- De privacy gerelateerde effecten moet geïdentificeerd en aangepakt worden.
- Incidenten met betrekking tot privacy worden gedetecteerd en afgehandeld
- Medewerkers toegang hebben tot de gegevens zijn competent en getraind in de privacy wetgeving.
- De entiteit informeert betrokkenen op transparante wijze over het beleid, de voorwaarden en activiteiten met betrekking tot het verzamelen, gebruiken, bewaren, verstrekken en verwijderen van persoonsgegevens.

- Er moet toestemming zijn voor het gebruik van de data van de betrokkenen
- De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt.
- Persoonsgegevens worden niet verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit
- De entiteit neemt bij het ontwikkelen en wijzigen van OMA het privacy-beleid, de privacy-principes en/of de van toepassing zijnde wet- en regelgeving in acht.
- De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken.
- Inzage, rectificatie, het wissen en een verzoek tot overdracht moet altijd op de juiste manier worden afgehandeld en moet mogelijk zijn voor de betrokkenen.
- Bij verwerving van data van derden wordt er voldoende aandacht besteed aan privacyoverwegingen en -vereisten
- De data moet binnen Nederland blijven of binnen landen met soortgelijke privacy wetten.
- Persoonsgegevens worden adequaat beschermd tegen onopzettelijke fouten of verlies, of kwaadwillige handelingen zoals hacken, diefstal, ongeautoriseerde verstrekking of verlies.
- Toegangsrechten worden adequaat toegekend, gewijzigd en ingetrokken.
- Door beperkte toegang tot persoonsgegevens tijdens verzending wordt op adequate wijze ongeautoriseerde verstrekking, inbreuk, wijziging of verwijdering van persoonsgegevens voorkomen.
- Inbreuk in verband met persoonsgegevens/datalek (onopzettelijk verlies of kwaadwillige handelingen zoals diefstal, ongeautoriseerde verstrekking of verlies) wordt voorkomen door middel van versleuteling.
- Toegang of toegangspogingen tot persoonsgegevens door medewerkers en derden worden geregistreerd en onderzocht om (pogingen tot) inbreuk op de beveiliging van persoonsgegevens te detecteren en te voorkomen.
- Systematische en periodieke evaluatie van privacyprocessen en beheersingsmaatregelen waarborgt dat deze naar behoren werken, zodat blijvend wordt voldaan aan de van toepassing zijnde wet- en regelgeving.

2.1.2.1 advies

Om de app te bouwen zal er dus eerst gekeken moeten worden naar de ''gewone'' persoonsgegevens en of de app gebouwd kan worden met alleen de ''gewone'' gegevens. Als dat niet het geval is mag er gekeken worden naar de ''bijzondere'' persoonsgegevens. Bijvoorbeeld het medisch dossier mag alleen gebruikt worden als er toestemming van de betrokkenen verstrek is. Verder moet de data noodzakelijk zijn voor de perfomance van de app anders mag het niet gebruikt worden. Verder moeten er punten doorlopen en nageleeft worden voordat de app gebouwd mag worden. Er wordt geadviseerd om aan de volledige lijst met punten te houden van het PCF om zo veel mogelijk risico's te voorkomen.

Het is nodig om op te merken dat er in de AVG en in het PCF staat beschreven dat er wettelijke grondslag nodig is voor het gebruiken van (bijzondere) persoonsgegevens. Dit betekend in het geval van OMA, dat er uitdrukkelijke toestemming van de betrokken nodig is. Verder moet er gekeken worden naar of de app het vitale belang beschermt van de betrokken. Hierbij staat beschreven dat de app essentieel is voor iemands leven of gezondheid moet zijn. Hierbij is essentieel het woord waar goed gekeken naar moet worden. Dit is niet in deze audit gebeurd en geven wij IT-Workz het advies om hier goed naar te kijken. Als er een conclusie wordt getrokken of de app essentieel is, dan kan de app ontworpen worden.

De punten uit het PCF die eerst behandeld moeten worden zijn: Het toestemmingsraamwerk → Identificatie en classificatie van persoonsgegevens → Minimale gegevensbewerking → Gebruik en beperkingen. Ook de maatregelen die bij iedere doelstelling horen moeten op de juiste volgorde afgewerkt worden. Voor een uitgebreidere beschrijving over dit alles zie hoofdstuk 3.1.2.

2.1.3 Deelvraag 3

2.1.3.1 Bevindingen

Deelvraag 3 luidt: *Hoe kan IT-Workz ervoor zorgen dat de data veilig opgeslagen wordt?*

Voor deze deelvraag wordt er wederom gebruik gemaakt van het PCF. In het PCF zijn er een vijftal beheersingsdoelstellingen onder het kopje “Gebruiken, opslaan en verwijderen”. Drie hiervan gaan concreet over het opslaan en zijn dus direct relevant voor deze deelvraag. Eén hiervan gaat over het verwijderen van data, en is dus indirect relevant voor de deelvraag. De laatste gaat over het gebruik van de gegevens. Dit is ten eerste niet gerelateerd aan de deelvraag en ten tweede is er technische informatie nodig over de OMA app om hier een uitspraak over te kunnen doen. Deze informatie ontbreekt momenteel helaas omdat de blauwdrukken nog worden opgesteld.

Dus de beheersingsdoelstellingen zijn:

- Doelbinding;
- Privacy architectuur;
- Bewaren van gegevens;
- Verwijdering, vernietiging en anonimisatie;
- Gebruik en beperking (niet gebruikt)

Per beheersingsdoelstelling zijn er meerdere beheersmaatregelen. Hierbij geldt het dringende advies voor IT-Workz om deze beheersmaatregelen op te volgen gedurende de implementatie en het onderhoud van de OMA app. De volledige lijsten met beheersingsdoelstellingen en beheersmaatregelen over het onderdeel “Gebruiken, opslaan en verwijderen” is te vinden in onderdeel 3.1.3.

Ten eerste is er **doelbinding**, wat inhoudt dat persoonsgegevens niet mogen worden verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij de betrokkene toestemming verleent of dit wettelijk vereist is. De bijbehorende beheersmaatregelen zijn:

a. *De entiteit richt een proces en procedures in om:*

    a. *De verstrekking en het gebruik van persoonsgegevens te beperken tot de gerechtvaardigde doeleinden die worden genoemd in het privacybeleid en de privacyverklaring van de entiteit;*
    b. *Bij voortduring te waarborgen dat de verstrekking en het gebruik van persoonsgegevens overeenkomstig de toestemming van de betrokkene en de betreffende wet- en regelgeving is.*
b. *In het privacybeleid van de entiteit is opgenomen dat doelbinding een privacyprincipe is.*

Ten tweede is er **privacyarchitectuur**, wat inhoudt dat de entiteit bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het solide privacybeleid, de privacyprincipes en/of de van toepassing zijnde wet- en regelgeving in acht neemt. De bijbehorende beheersmaatregel is:

a. *Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten waarbij persoonsgegevens worden verwerkt, houdt de entiteit zo vroeg mogelijk in het ontwerpproces rekening met de privacyprincipes en privacyrisico's. Het risico op strijdigheid tussen het ontwerp en de rechten en vrijheden van betrokkenen (en het privacybeleid van de entiteit) is geïdentificeerd en aangepakt.*
b. *De beoordeling van privacyrisico's is een inherent en gedocumenteerd onderdeel van de projectmethodiek en/of het ontwikkelingsproces van de entiteit.*
c. *Wanneer systemen, diensten en producten waarbij persoonsgegevens worden verwerkt privacy-gerelateerde opties bieden, zijn deze standaard ingesteld op de meest beperkende optie met betrekking tot privacy.*

Als derde is er het **bewaren van gegevens**, wellicht de meest belangrijke voor OMA. Het houdt in dat persoonsgegevens niet langer worden bewaard dan noodzakelijk, dan wettelijk is toegestaan of dan noodzakelijk is voor de doeleinden waarvoor zij werden verzameld. De bijbehorende beheersmaatregelen zijn:

a. *De entiteit:*
    a. *Documenteert het bewaarbeleid en de verwijderingsprocedures ten aanzien van persoonsgegevens;*
    b. *Zorgt dat persoonsgegevens niet langer worden bewaard dan de vastgestelde bewaartermijn, tenzij er sprake is van een gerechtvaardigde reden of wettelijke verplichting.*
    c. *Documenteert voor elke verwerking van persoonsgegevens de betreffende bewaartermijn;*
    d. *Informeert betrokkenen in de privacyverklaring over het beleid ten aanzien van bewaartermijnen;*
    e. *Slaat gearchiveerde kopieën en back-ups op, bewaart en verwijdert deze overeenkomstig het bewaarbeleid;*
    f. *Instrueert verwerkers over bewaartermijnen.*
b. *Bij het vaststellen van bewaarprocedures worden wettelijke en contractuele bewaartermijnen in acht genomen; deze wijken mogelijk af van de normale beleidsregels.*

Ten slotte is er het onderdeel **verwijdering, vernietiging en anonimisatie**, wat inhoudt dat persoonsgegevens indien nodig worden geanonimiseerd en/of verwijderd binnen de entiteit. De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken. Dit is relevant wanneer gebruikers van OMA eisen dat data verwijderd wordt. Bovendien moet alle data überhaupt al geanonimiseerd zijn, zoals in deelvraag 2 wordt aangehaald. De bijbehorende beheersmaatregelen zijn:

a. *De entiteit heeft een gedocumenteerde procedure ingericht om te waarborgen dat:*
    a. *Het wissen en vernietigen van persoonsgegevens geschiedt conform het bewaarbeleid, ongeacht de vorm waarin deze zijn opgeslagen (zoals elektronisch, op optische media, of op papier);*
    b. *De verwijdering van originele, gearchiveerde gegevens, back-ups en persoonlijke kopieën conform het vernietigingsbeleid plaatsvindt;*
    c. *De verwijdering van persoonsgegevens op een adequate wijze wordt vastgelegd.*

    De entiteit zorgt er daarnaast voor dat:
    d. *Persoonsgegevens worden gelokaliseerd en verwijderd of teruggebracht, voor zover dit technisch mogelijk is.*
    e. *Persoonsgegevens die niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of gegevens die op grond van wet- en regelgeving moeten worden verwijderd, op regelmatige en systematische basis worden vernietigd, gewist of geanonimiseerd.*
b. *Bij het vaststellen van procedures voor verwijdering, vernietiging en vermindering van persoonsgegevens worden contractbepalingen in acht genomen indien deze afwijken van de normale beleidsregels.*

2.1.3.2 Advies

Het dringende advies voor IT-Workz geldt om al de beheersmaatregelen op te volgen om de beheersingsdoelstellingen te behalen. Daarbij hebben de eerste drie de hoogste prioriteit omdat deze gaan over het opslaan van de data. Het vierde onderdeel “verwijderen, vernietigen en anonimisatie” heeft daarentegen de laagste prioriteit omdat het indirect relevant is voor de deelvraag. Van de eerste drie beheersingsdoelstellingen heeft “bewaren van gegevens” de hoogste prioriteit. Deze bevat korte en duidelijke richtlijnen en grenzen over hoe en hoe lang de gegevens bewaard moeten worden. Per beheersingsdoelstelling kan er niet echt onderscheid gemaakt worden tussen de beheersmaatregelen, maar de maatregelen zijn wel op een redelijk chronologische manier opgesteld, dus het is aangeraden om deze volgorde aan te houden bij de uitwerking.

Kortom, IT-Workz wordt aangeraden om te beginnen bij de beheersingsdoelstelling “Bewaren van gegevens”. Hierna is het verstandig om de doelstellingen chronologisch te volgen, dus van boven naar beneden. Dat wil zeggen: Bewaren van gegevens → Doelbinding → Privacy architectuur → Verwijdering, vernietiging en anonimisatie. Ook de maatregelen die bij iedere doelstelling horen moeten op de juiste volgorde afgewerkt worden. Voor een uitgebreidere beschrijving over dit alles zie hoofdstuk 3.1.3.

2.2 Onderbouwing oordeel en prioritering

Om de app volgens de wet op te leveren wordt er aangeraden om eerst te kijken naar de data die nodig is. Hierbij moet er gekeken worden naar welke data noodzakelijk is voor de app en welke datapunten toegevoegde waarde hebben maar niet noodzakelijk zijn. Als volgt, zal er gekeken moeten worden naar de klasse van de data. Welke punten zijn bijzondere data en welke niet. Hier zal dan de maatregels van het PCF tegenaan gelegd moeten worden. Daarna moeten de richtlijnen die in hoofdstuk 2.1.2 staan beschreven opgevolgd worden. Ten slotte moeten de beheersingsmaatregels van hoofdstuk 2.1.3 in behandeling genomen worden. Als deze punten in de benoemde volgorde gemaakt worden, zal het risico van dat de app binnen de AVG aanzienlijk afnemen.

3 Bijlagen

3.1 Werkwijze van uitvoering per stap

3.1.1 Deelvraag 1

Voorafgaand aan het opstellen van de datapunten is er veel contact geweest met de opdrachtgever van IT-Workz. Door in de beginfase duidelijkheid te vergaren over de werking van de OMA app is er veel inspiratie opgedaan over mogelijke datapunten. Ook heeft het projectteam inzage gekregen in een verzuimdocumentatie van SOML. Door middel van een korte **data analyse** is er ook inspiratie opgedaan over mogelijke datapunten. Door middel van een **brainstormsessie** is er een longlist opgesteld met alles wat mogelijk nuttig was voor OMA.

In een **expert interview** met de stakeholder Experience Data is deze lijst voorgelegd aan de expert. Hij is er met een kritisch oog overheen gegaan en heeft een aantal datapunten kunnen wegstrepen omdat ze niet nuttig waren voor OMA. Daarbij zijn er namen en omschrijvingen veranderd, of zijn sommige datapunten gegroepeerd omdat ze onder hetzelfde kopje passen. Tevens heeft de expert advies gegeven over welke data wel en niet gebruikt mag worden, maar dit komt terug in onderdeel 3.1.2 Deelvraag 2.

3.1.2 Deelvraag 2

Om vast te kunnen stellen welke maatregelingen er zijn binnen het PCF is het PCF volledig doorgelezen zodat het framework volledig begrepen is door de auditors. Daarna is er meer **literatuur studie** gedaan door de term “bijzondere persoonsgegevens” te onderzoeken. Door de variabelen dan onder te verdelen in bijzondere persoonsgegevens en gewone persoonsgegevens kan er gekeken worden naar de wetgeving voor de variabelen. Het verdelen van de variabelen is gedaan door middel van een **brainstorm sessie**. In de brainstorm sessie is er ook besproken hoe de maatregels het beste aan de variabelen gekoppeld kunnen worden.

Alle bevindingen gaan gevalideerd worden door middel van een **expert interview** met professionals van Experience Data. Hierbij moet wel vermeld worden dat er een belang is bij deze expert. Dit komt omdat experience data de app zal gaan ontwikkelen. Verder heeft een security specialist van IT-Workz naar gekeken. Ook IT-workz heeft belang naar het maken van de app. Als verantwoordelijke van de app zal deze expert er grondig naar hebben gekeken.

Omdat er in hoofdstuk 2.1.2 alleen een samenvatting staat van de belangrijkste punten staan, is er hieronder de volledige lijst te vinden met de specifieke maatregels uit het PCF opgesteld. Hier is verder de punten uit de AVG-wetgeving toegevoegd voor duidelijkheid.

Welke data mag er verzameld en gebruikt worden volgens het passende AVG-raamwerk?

In de AVG wetgeving wordt er onderscheid gemaakt tussen persoonsgegevens en speciale/bijzondere persoonsgegevens. Bij het project OMA zal er gebruik gemaakt worden van beide types. Het is daarom belangrijk om te weten wat het verschil is tussen beiden.

Persoonsgegevens: *"Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die*

kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon." (FG Support. z.d.)

Bijzondere/speciale persoonsgegevens: *'' Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze 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''* (Vollmer, N. 2020, 22 mei)

Er is verder nog een uitzondering en dit is het verwerken van persoonsgegevens van kinderen. Hieronder vindt u de regel over persoonsgegevens van kinderen.

Persoonsgegevens van kinderen: *"Verwerkt een organisatie straks gegevens van kinderen online? Bijvoorbeeld via een app, online game, webwinkel of via sociale media? Dan mag dit bij kinderen onder de 16 jaar alleen als de ouders hiervoor toestemming hebben gegeven. Organisaties moeten ook controleren of die toestemming daadwerkelijk is gegeven." (Mag ik onder de AVG gegevens van kinderen verwerken?* z.d.)

De datapunten uit deelvraag 1 kunnen dus onderverdeeld worden tussen het type persoonsgegevens. De variabelen gegevens over medische klachten en het vaccinatiepaspoort vallen onder de bijzondere persoonsgegevens. Onder de gegevens van de klas kunnen persoonsgegevens van kinderen omvatten. De rest van de gegevens zijn ''gewone'' persoonsgegevens.

Nu dat de data type bekend zijn kan er gekeken worden naar de verschillende data type en wat er volgens het NOREA PCF verzameld en gebruikt mag worden.

Voor bijzondere persoonsgegevens:

De wet voor bijzondere persoonsgegevens:

- Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze 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.
- Dit is niet van toepassing wanneer aan een van de onderstaande voorwaarden is voldaan:
    - Iemand heeft uitdrukkelijk toestemming gegeven voor de verwerking van zijn/haar persoonsgegevens.
    - (*alleen als het in een wet staat*) De verwerking is noodzakelijk om verplichtingen uit te voeren of specifieke rechten uit te oefenen van u of de betrokken persoon. Dit op het gebied van het arbeidsrecht, het socialezekerheidsrecht en het sociale beschermingsrecht.
    - De verwerking is noodzakelijk om de vitale belangen van de betrokken persoon of van een andere natuurlijke persoon te beschermen. Dit geldt alleen wanneer diegene fysiek of juridisch niet in staat is om zijn/haar toestemming te geven.
    - U verwerkt de gegevens als stichting, vereniging of andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is. Het gaat om gegevens van uw (oud)leden of personen met wie u regelmatig contact heeft gerelateerd aan uw doelstelling. En u verwerkt de gegevens voor gerechtvaardigde activiteiten en met passende waarborgen.

- U verwerkt persoonsgegevens die de betrokkene zelf doelbewust openbaar heeft gemaakt.
- De verwerking is noodzakelijk om een rechtsvordering in te stellen, uit te oefenen of te onderbouwen. Of u handelt als gerecht vanuit uw rechtsbevoegdheid.
- (*alleen als het in een wet staat*) De verwerking is noodzakelijk voor een zwaarwegend algemeen belang.
- (*alleen als het in een wet staat*) De verwerking is noodzakelijk voor doeleinden van preventieve of (arbeids)geneeskundige aard. Zoals het beoordelen van arbeidsgeschiktheid en/of het verstrekken van gezondheidszorg.
- (*alleen als het in een wet staat*) De verwerking is noodzakelijk voor de volksgezondheid.
- (*alleen als het in een wet staat*) De verwerking is noodzakelijk voor archivering in het algemeen belang, wetenschappelijk/historisch onderzoek of statistische doeleinden.

(Mag u persoonsgegevens verwerken? z.d), (Vollmer, N. 2020b, mei 22)

Volgens het PCF:

CFR03	De entiteit verzamelt of verwerkt geen bijzondere categorieën van persoonsgegevens, tenzij de entiteit hiervoor een wettelijke grondslag heeft. Wanneer de uitdrukkelijke toestemming van de betrokkene de wettelijke grondslag is voor de verwerking van bijzondere categorieën van persoonsgegevens, heeft de betrokkene door middel van een duidelijke actieve handeling ingestemd met het gebruik of de verstrekking van bijzondere categorieën van persoonsgegevens. De entiteit verkrijgt de uitdrukkelijke toestemming rechtstreeks van de betrokkene en documenteert/bewaart het bewijs dat deze toestemming is verleend, bijvoorbeeld door de persoon te vragen een vakje aan te vinken of een formulier te ondertekenen.
PDI02	De entiteit maakt duidelijk onderscheid tussen de verwerking van (a) persoonsgegevens en (b) bijzondere categorieën van persoonsgegevens.
PDI03	De entiteit heeft een procedure opgesteld om te bepalen of bij bestaande of geplande verwerking van persoonsgegevens bijzondere categorieën van persoonsgegevens worden verwerkt. Als dit het geval is, wordt de rechtmatigheid van de (geplande) verwerking uitvoerig beoordeeld en gedocumenteerd en worden maatregelen getroffen om veilige verwerking volgens de geldende voorschriften te waarborgen.

Tabel 2: Benodigdheden voor bijzondere persoonsgegevens

Voor de "gewone" persoonsgegevens:

Volgens de wet:

Er moet een goede reden zijn om persoonsgegevens te verwerken. In de privacywet, de Algemene Verordening Gegevensbescherming (AVG), staan 6 redenen genoemd. De juridische naam voor die redenen is grondslagen. U heeft dus een grondslag nodig om persoonsgegevens te mogen

verwerken. Let op: u moet zelf beoordelen welke grondslag voor u van toepassing is. Dat is uw eigen verantwoordelijkheid. U bepaalt de grondslag voordat u begint met gegevens te verwerken. In de AVG staan de volgende 6 grondslagen voor het verwerken van persoonsgegevens:

- 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.

Volgens het PCF:

Verzamelen

Minimale gegevensverwerking (DMI) *Beheersingsdoelstelling:* De persoonsgegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de gerechtvaardigde doeleinden waarvoor zij worden verwerkt.		
Fase informatielevenscyclusmanagement: **Verzamelen**		
Beheersingsmaatregelen:		
DMI01	De entiteit richt een proces en procedures in om: a. te bepalen welke persoonsgegevens noodzakelijk zijn voor het doel van de verwerking en welke persoonsgegevens optioneel zijn; b. de verwerking van persoonsgegevens te beperken tot het voor het doel noodzakelijke minimum; c. periodiek na te gaan of de verwerking van persoonsgegevens nog noodzakelijk is voor de producten en/of diensten van de entiteit.	VV
DMI02	In het privacybeleid van de entiteit is opgenomen dat minimale gegevensverwerking een privacyprincipe is (zie PPO).	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Gegevensbescherming door ontwerp / door standaardinstellingen		

Tabel 3: Minimale gegevensverwerking

Gebruik en beperking (URE)		
Beheersingsdoelstelling: Persoonsgegevens worden niet verwerkt als de betrokkene een beperking van de verwerking heeft verkregen of wanneer er sprake is van specifieke juridische restricties door lokale autoriteiten. Bezwaren van de betrokkene tegen de verwerking van persoonsgegevens worden op een adequate wijze afgehandeld.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
~~URE01~~	*Samengevoegd met PST01.*	
URE02	De entiteit heeft een proces ingericht om adequaat te handelen wanneer betrokkenen hun recht op beperking van of bezwaar tegen de verwerking uitoefenen.	VV
URE03	De entiteit heeft vastgesteld of lidstaatrechtelijke bepalingen de verwerking van persoonsgegevens beperken (bijvoorbeeld ter bescherming van de nationale of openbare veiligheid) en kan aantonen dat deze beperkingen worden gehandhaafd.	VV
PST01	In de privacyverklaring van de entiteit staat: a. welke persoonsgegevens worden verzameld, waar deze informatie vandaan komt, de doeleinden voor de verzameling en de betreffende rechtsgronden voor de verwerking; b. wat de gevolgen zijn, voor zover daar sprake van is, als de betrokkene de gevraagde gegevens niet verstrekt; c. informatie over verdere verwerking (indien van toepassing); d. informatie over de rechten van betrokkenen en de wijze waarop zij die rechten kunnen uitoefenen (zie ook URE, DAR, DCR, DDR, DPR).	VV

Tabel 4: Gebruik en beperking

3.1.3 Deelvraag 3

In deelvraag 2 is er gekeken naar welke data wel en niet opgeslagen en gebruikt mogen worden. In deelvraag 3 wordt er naar een specifiek onderdeel van het PCF gekeken, namelijk het hoofdstuk “Gebruiken, opslaan en verwijderen”. Dit bevat verschillende beheersingsdoelstellingen die ieder onderverdeeld zijn in meerdere beheersingsmaatregelen. Degenen die van toepassing zijn op deze audit zijn in Tabel 5, 6, 7 en 8 terug te vinden.

Doelbinding (ULI) *Beheersingsdoelstelling:* Persoonsgegevens worden niet verstrekt, beschikbaar gesteld of anderszins voor andere doeleinden gebruikt dan die zijn geformuleerd in de privacyverklaring van de entiteit, tenzij: • de betrokkene toestemming verleent; of • dit wettelijk vereist is.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
ULI01	De entiteit richt een proces en procedures in om: a. de verstrekking en het gebruik van persoonsgegevens te beperken tot de gerechtvaardigde doeleinden die worden genoemd in het privacybeleid en de privacyverklaring van de entiteit; b. bij voortduring te waarborgen dat de verstrekking en het gebruik van persoonsgegevens overeenkomstig de toestemming van de betrokkene en de betreffende wet- en regelgeving is.	VV
ULI02	In het privacybeleid van de entiteit is opgenomen dat doelbinding een privacyprincipe is (zie PPO).	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Gegevensbescherming door ontwerp / door standaardinstellingen		

Tabel 5: Doelbinding

Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaardinstellingen) (PBD) *Beheersingsdoelstelling:* De entiteit neemt bij het ontwikkelen en wijzigen van producten, diensten, bedrijfssystemen of processen het solide privacybeleid, de privacyprincipes en/of de van toepassing zijnde wet- en regelgeving in acht.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
PBD01	Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten waarbij persoonsgegevens worden verwerkt, houdt de entiteit zo vroeg mogelijk in het ontwerpproces rekening met de privacyprincipes en privacyrisico's. Het risico op strijdigheid tussen het ontwerp en de rechten en vrijheden van betrokkenen (en het privacybeleid van de entiteit) is geïdentificeerd en aangepakt. Wanneer de entiteit diensten van derden bij deze activiteiten betrekt, verplicht de entiteit deze partijen om dezelfde risicomanagementactiviteiten ten aanzien van privacy te hanteren.	VV
PBD02	De beoordeling van privacyrisico's is een inherent en gedocumenteerd onderdeel van de projectmethodiek en/of het ontwikkelingsproces van de entiteit.	VV
PBD03	Wanneer systemen, diensten en producten waarbij persoonsgegevens worden verwerkt privacy-gerelateerde opties bieden, zijn deze standaard ingesteld op de meest beperkende optie met betrekking tot privacy.	VV
Gerelateerde kernelementen van de AVG: • Gegevensbescherming door ontwerp / door standaardinstellingen • Privacyprincipes		

Tabel 6: Privacyarchitectuur

Bewaren van gegevens (DRE) *Beheersingsdoelstelling:* Persoonsgegevens worden niet langer bewaard dan noodzakelijk, dan wettelijk is toegestaan of dan noodzakelijk is voor de doeleinden waarvoor zij werden verzameld.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
DRE01	De entiteit: a. documenteert het bewaarbeleid en de verwijderingsprocedures ten aanzien van persoonsgegevens; b. zorgt dat persoonsgegevens niet langer worden bewaard dan de vastgestelde bewaartermijn, tenzij er sprake is van een gerechtvaardigde reden of wettelijke verplichting. c. documenteert voor elke verwerking van persoonsgegevens de betreffende bewaartermijn; d. informeert betrokkenen in de privacyverklaring over het beleid ten aanzien van bewaartermijnen; e. slaat gearchiveerde kopieën en back-ups op, bewaart en verwijdert deze overeenkomstig het bewaarbeleid; f. instrueert verwerkers over bewaartermijnen.	VV
DRE02	Bij het vaststellen van bewaarprocedures worden wettelijke en contractuele bewaartermijnen in acht genomen; deze wijken mogelijk af van de normale beleidsregels.	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker		

Tabel 7: Bewaren van gegevens

Verwijdering, vernietiging en anonimisatie (DDA)		
Beheersingsdoelstelling: Persoonsgegevens worden indien nodig geanonimiseerd en/of verwijderd binnen de entiteit. De identiteit van personen kan niet worden herleid en persoonsgegevens zijn niet meer beschikbaar nadat de bewaartermijn is verstreken.		
Fase informatielevenscyclusmanagement: **Gebruiken, opslaan en verwijderen**		
Beheersingsmaatregelen:		
DDA01	De entiteit heeft een gedocumenteerde procedure ingericht om te waarborgen dat: a. het wissen en vernietigen van persoonsgegevens geschiedt conform het bewaarbeleid, ongeacht de vorm waarin deze zijn opgeslagen (zoals elektronisch, op optische media, of op papier); b. de verwijdering van originele, gearchiveerde gegevens, back-ups en persoonlijke kopieën conform het vernietigingsbeleid plaatsvindt; c. de verwijdering van persoonsgegevens op een adequate wijze wordt vastgelegd. De entiteit zorgt er daarnaast voor dat: d. persoonsgegevens worden gelokaliseerd en verwijderd of teruggebracht, voor zover dit technisch mogelijk is. e. persoonsgegevens die niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of gegevens die op grond van wet- en regelgeving moeten worden verwijderd, op regelmatige en systematische basis worden vernietigd, gewist of geanonimiseerd.	VV
DDA02	Bij het vaststellen van procedures voor verwijdering, vernietiging en vermindering van persoonsgegevens worden contractbepalingen in acht genomen indien deze afwijken van de normale beleidsregels.	VV
Gerelateerde kernelementen van de AVG: • Privacyprincipes • Verantwoordelijkheden van verwerkingsverantwoordelijke en verwerker • Beveiliging van de verwerking • Gegevensbescherming door ontwerp / door standaardinstellingen		

Tabel 8: Verwijdering,vernietiging en anonimatie

3.2 Beschrijving organisatie en systeem

IT-Workz is een ICT dienstverlener voor verschillende onderwijsinstellingen. Om kwalitatieve diensten te verlenen aan zijn klanten moeten deze diensten aan de hoogste kwaliteitsvoorwaarden voldoen. Hiervoor is het belangrijk dat er een IT-Audit uitgevoerd wordt op de toekomstige diensten die IT-Workz aan hun klanten willen gaat bieden. IT-Workz heeft zelf geen programmeurs in dienst die ervaring heeft met het bouwen van machine learning algoritmes, daarom hebben ze Experience Data ingehuurd om de OMA applicatie te bouwen.

Experience Data is gespecialiseerd in het bouwen van “Artificial Assistance” applicaties die actiegerichte aanbevelingen voor repetitieve en complexe activiteiten uitvoert.

3.3 Lijst met auditees

Auditees	Betrokkenheid
IT-Workz	IT-Workz is een organisatie die ICT-dienstverleningen aan onderwijsinstellingen biedt. IT-Workz heeft zelf geen ervaring met het bouwen van machine learning algoritmes daarom hebben ze besloten om de applicatie door Experience data laten bouwen. Deze audit wordt uitgevoerd in opdracht van IT-Workz. De rol van IT-Wokz is om de auditors te voorzien van voldoende informatie zodat zij de audit kunnen uitvoeren. IT-Workz staat als contactpunt tussen de auditors en de andere organisaties die deel maken aan deze audit. Het resultaat en het advies van de audit zal aan IT-Workz worden geleverd.
SOML	Stichting Onderwijs Midden-Limburg (SOML) is een scholengemeenschap met meer dat 860 personeelsleden gevestigd in midden-Limburg. SOML zal een van de eindgebruikers zijn voor de OMA-applicatie. De beschikbare data die gebruikt zal worden tijdens het bouwen van de OMA-applicatie zal door SOML verzorgd.
Experience data	Experience data is een bedrijf met creatieve analisten die complexe vraagstukken aanpakken. Experience data zorgt voor toepassingen die helpen bij het oplossen van compleze vraagstukken met behulp van ervaringsgegevens. Experience data zal de OMA-applicatie voor IT-Workz bouwen en beheren. Omdat de Audit in het begin van het project plaatsvindt zullen de auditors onderzoeken welke gegevens gebruikt kunnen worden. Experience data zal de auditors tijdens het onderzoek helpen door hun kennis en ervaringen ter beschikking te stellen. Door interviews te plegen met de deskundigen van Experience data kan de auditors een beter inzicht krijgen in de functionaliteiten van de Oma applicatie.

Tabel 9: Lijst met auditees

3.4 Begrippenlijst

Begrippen	Definitie/ verklaring
Kunstmatige intelligentie	Kunstmatige intelligentie verwijst naar elke mensachtige intelligentie die wordt vertoond door een computer, robot of andere machine. In de volksmond verwijst kunstmatige intelligentie naar het vermogen van een computer of machine om de mogelijkheden van de menselijke geest na te bootsen - leren uit voorbeelden en ervaring, voorwerpen herkennen, taal begrijpen en erop reageren, beslissingen nemen, problemen oplossen - en deze en andere mogelijkheden te combineren om functies uit te voeren die een mens zou kunnen uitvoeren, zoals een hotelgast begroeten of een auto besturen. (Education, I. C. 2021b, 7 april)
Machine learning	Machine learning is een tak van kunstmatig intelligentie (AI) die zich toelegt op het bouwen van toepassingen die van gegevens leren en hun nauwkeurigheid in de loop van de tijd verbeteren zonder daartoe geprogrammeerd te zijn. (Education, I. C. 2021, 25 maart).
Betrokkene	In de context van het PCF zijn de betrokkenen degenen wiens data wordt opgeslagen/gebruikt/verwijderd.
Entiteit	In de context van het PCF is de entiteit de partij/organisatie die de gegevens opslaat, maar niet degene die de gegevens verwerkt.
Gegevensverwerker	De gegevensverwerker is het onderdeel van de entiteit die zich bezig houdt met de verwerking van de data.

Tabel 10: Begrippenlijst

3.5 Lijst met afkortingen

Afkorting	Uitleg
PCF	Privacy Control Framework
OMA	Operationeel Onderwijs Assistent
NOREA	De Nederlandse Orde van Register EDP-Auditors
SOML	Stichting onderwijs midden-Limburg
AVG	Algemene vordering gegevensbescherming
AI	Kunstmatige intelligentie
ML	Machine learning
DPIA	Data protection impact assessment
DDA	Verwijdering, Vernieteging en anonimisatie
DRE	Bewaren van gegevens
PBD	Privacy architectuur (Gegevensbescherming door ontwerp en door standaardinstellingen)
ULI	Doelbinding
URE	Gebruik en beperking
PST	Privacyverklaring
PDI	Identificatie en classificatie van persoonsgegevens
CFR	Toestemmingsraamwerk
DMI	Minimale gegevenswerking

Tabel 11: Lijst met afkortingen

3.6 Literatuurlijst

- De Heer, J. (2019, 1 augustus). NOREA Handreiking Privacy Control Framework. Geraadpleegd op 22 april 2021, van https://www.norea.nl/download/?id=6317
- NOREA - de beroepsorganisatie van IT-Auditors. (z.d.). Geraadpleegd op 22 april 2021, van https://www.norea.nl/nieuws/4172/avg-privacy-control-framework-gepubliceerd
- Education, I. C. (2021, 25 maart). Machine Learning. Geraadpleegd op 20 april 2021, van https://www.ibm.com/cloud/learn/machine-learning
- Education, I. C. (2021b, 7 april). Artificial Intelligence (AI). Geraadpleegd op 20 april 2021, van https://www.ibm.com/cloud/learn/what-is-artificial-intelligence
- FG Support. (z.d.). Wat verstaat de AVG onder (bijzondere) persoonsgegevens. Geraadpleegd op 29 april 2021, van https://www.fgsupport.nl/wat-zijn-persoonsgegevens
- Vollmer, N. (2020, 22 mei). Artikel 9 EU algemene verordening gegevensbescherming (EU-AVG). Privacy/Privazy according to plan. Nicholas Vollmer. https://www.privacy-regulation.eu/nl/artikel-9-verwerking-van-bijzondere-categorieen-van-persoonsgegevens-EU-AVG.htm
- Mag ik onder de AVG gegevens van kinderen verwerken? (z.d.). Autoriteit Persoonsgegevens. Geraadpleegd op 29 april 2021, van https://autoriteitpersoonsgegevens.nl/nl/nieuws/mag-ik-onder-de-avg-gegevens-van-kinderen-verwerken
- *Mag u persoonsgegevens verwerken?* (z.d.). Autoriteit Persoonsgegevens. Geraadpleegd op 30 april 2021, van https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/mag-u-persoonsgegevens-verwerken#wanneer-mag-u-bijzondere-persoonsgegevens-verwerken-6341
- Vollmer, N. (2020b, mei 22). *Artikel 9 EU algemene verordening gegevensbescherming (EU-AVG). Privacy/Privazy according to plan.* Nicholas Vollmer. https://www.privacy-regulation.eu/nl/artikel-9-verwerking-van-bijzondere-categorieen-van-persoonsgegevens-EU-AVG.htm
- Schoemaker, R. (2021, 21 mei). *Nog een privacy control framework om de AVG te borgen?* Informatiebeveiliging & Privacy. https://ib-p.nl/2019/01/nog-een-privacy-control-framework-om-de-avg-te-borgen/

3.7 Figuren- en Tabellenlijst

3.8 Norea PCF Framework (PDF)

Het Norea PCF Framework is het framework dat in dit document wordt gebruikt. De Norea PCF Framework kan u op deze link downloaden. Als extra hebben we de PDF als een “embedded file” toegevoegd.

090919 NOREA
Privacy Control Frame

3.9 Onderzoek frameworks

Tijdens het zoeken naar frameworks die gebruikt kunnen worden is er gekeken naar verschillende frameworks. Hieronder vindt u de lijst met onderzochte frameworks.

Onderzochte methodes:

- Wet bescherming persoonsgegevens (Wbp)
- GAPP (AICPA/CICA).
- SP800-R53 Privacy Control Catalog (NIST).
- Het privacy control framework
- European Privacy Seal (EuroPriSe) raamwerk.

Er is de keuze gemaakt voor de meest relevante frameworks kiezen. Dit is gedaan door de minst relevante elke keer weg te strepen. Het Wbp is niet gekozen omdat de wet niet meer in gebruik is. De GAPP is een Canadese framework en is dus minder relevant, dit geldt ook voor de NIST. De European privacy seal is een seal die bedrijven krijgen als ze voldoen aan de GDPR. Dit betekent dat het PCF overblijft. Hieronder vindt u het onderzoek naar van welk bedrijf we het PCF wilde gebruiken

- Het NOREA Privacy Control Framework – Het primaire doel van het PCF van NOREA is het bieden van een handreiking aan (audit) professionals bij het beoordelen of de controledoelstellingen van een organisatie met betrekking tot privacy en bescherming van persoonsgegevens worden bereikt. Het PCF bevat de voorgeschreven doelstellingen en elementen voor privacy-opdrachten op basis van de NOREA Assurance richtlijn 3000.

- De Privacy Baseline van het CIP – Het primaire doel van de Privacy Baseline van het CIP is het vertalen van AVG eisen naar concrete, hanteerbare normen die duidelijk maken wat organisaties moeten doen om in overeenstemming met de wet de privacy van de betrokkenen te waarborgen. De baseline van het CIP volgt hierbij de SIVA methodiek en is daarmee ook geschikt als auditcriteria. Daarnaast biedt het CIP interessante ondersteuningsproducten op het gebied van privacymanagement (zie blog ‘De privacy menukaart van het CIP’).

- Het Privacy Control Framework van VNG – ook wel ‘Criteria borging AVG’ genoemd. Het primaire doel van deze VNG borgingscriteria is om gemeenten concrete handvatten te bieden om een goede omgang met persoonsgegevens in de gehele organisatie te waarborgen. VNG Realisatie heeft daarom criteria ontwikkeld om de AVG te vertalen naar

een kwaliteitscyclus voor gegevensbescherming en privacy, specifiek voor gemeentelijke processen. Deze criteria zijn ook in Excel formaat te downloaden vanaf de VNG Realisatie website.[1]

Uit de 3 keuzes is er gekozen voor het NOREA PCF. Dat komt omdat de NOREA een internationaal erkende audittors organisatie is met veel kennis. Daarbij sluit het PCF nauw aan op de 13 kernelementen van de AVG. Het PCF heeft verder een goede overlap met de NEN-ISO/IEC ISO 27001 en 27002 normenkaders. (De Heer, J. 2019, 1 augustus). Er was niet voor het VNG gekozen omdat het VNG gemaakt is voor gemeentes.

3.10 Overige opmerkingen

Hieronder vindt u een lijst met opmerkingen die zijn gemaakt door de security specialist van IT-Workz. Deze opmerkingen hebben we in het document proberen te plaatsen indien het pasten. Deze opmerkingen vonden wij belangrijk dat die meegenomen moeten worden als de app gebouwd gaat worden. De opmerkingen zijn als volgt:

1. Het is van belang dat data versleuteld is. Versleuteling is belangrijk voor data in transit en at rest. Hier moet goed over nagedacht worden en mogelijk moet ook nagedacht worden over scheiding tussen de applicatie systemen en de database(s) waar de data opgeslagen wordt.
2. Gaat er inderdaad historische data gebruikt worden? Dit zou dan betekenen dat oudere verzuimdata mogelijk wordt opgevraagd en ook opgeslagen wordt in de database, klopt dat? Indien dat zo is, dan plaats ik de kanttekening dat het de vraag is of dit wel mag.
3. Uit welk systeem of systemen komt de data? Welke koppelingen met systemen zouden er gerealiseerd moeten worden om deze data te verkrijgen?
4. Wanneer iemand toestemming heeft gegeven om de data te verzamelen, verwerken en bewaren, en die persoon bedenkt zich, kan de toestemming dan via een web portal, de app of op een andere manier snel worden ingetrokken of is dit een proces waar aanzienlijk wat tijd over heen gaat?
5. Data zal na een bepaalde termijn verwijderd moeten worden. Hoe controleer je dit en hoe kun je dit zo inregelen dat dit geautomatiseerd plaats kan vinden?
6. Incidenten met betrekking tot privacy moeten worden gedetecteerd en worden afgehandeld. Hoe wordt deze detectie/monitoring ingeregeld? Hoe wordt gedetecteerd dat er mogelijk data is gelekt? Wie gaan de privacy incidenten registreren, oppakken en afhandelen?
7. Advies 1: Indien IT-Workz de privacy incidenten zou moeten gaan registreren, oppakken en afhandelen is het advies om dit te borgen in het (security) incident managementproces. Zorg er dan voor dat er incident scenario's zijn en playbooks en hoe een incident afgehandeld moet worden.
8. Advies 2: Indien IT-Workz de monitoring en detectie in moet regelen, dan moet heel goed gekeken worden wat er precies gemonitord moet worden en waar detectie op moet worden ingericht. Denk aan het kunnen detecteren van data die vanuit de database naar buiten wordt verstuurd, data dumps (kopiëren en/of verplaatsen van data) of bijvoorbeeld een grote hoeveelheid aan data die ineens verwijderd wordt.
9. Op pagina 9 wordt de privacy architectuur benoemd; privacy by design moet de insteek zijn en dan komen er mogelijk nog aanvullende zaken om de hoek kijken om die privacy te garanderen. Het is voor IT-Workz de vraag of dit dan ook opgenomen moet worden in de

scope van audits. Patch- en vulnerability management zijn 2 belangrijke onderwerpen die dan terug komen en mogelijk is het een goed idee om regelmatig een penetration test uit te voeren.

10. Het doel voor het verzamelen van deze data is inzichtelijk te krijgen welke trends er zijn qua verzuimdata. Wie gaat deze informatie uiteindelijk gebruiken? Is dat de school zelf, de bedrijfsarts? Dit is een ethisch vraagstuk, omdat medische informatie geheim is en niet aan de werkgever hoeft te worden verstrekt. Het 'gevaar' zit hem mogelijk ook in de informatie die er uit komt en of dit (al dan niet geanonimiseerd) ter herleiden is naar 1 persoon. In een kleine organisatie zullen specifieke verzuimklachten mogelijk makkelijker te herleiden zijn naar 1 persoon. Hoe wordt daar dan mee omgegaan? Mag dit wel?
11. Van de genoemde grondslagen voor het mogen verzamelen, verwerken en opslaan van deze data, lijkt het op dit moment dat er geen van de genoemde grondslagen het rechtvaardigt om dit te mogen doen voor de OMA app.