14-5-2023

Onderzoek (AVG)

Nick Beun

Nick Beun | 512714
COMPETENTIE - ANALYSEREN

Samenvatting

Het verslag gaat over het onderzoek naar het nakomen van de Algemene Verordening Gegevensbescherming (AVG) en gegevensbescherming in relatie tot de ontwikkeling van een nieuwe applicatie voor de Dutch Dolphins Swimming Club. Verschillende onderzoeksmogelijkheden worden besproken, waaronder literatuurstudie, juridische analyse, case studie en ethiek- en privacy-impactbeoordeling. Het belang van het begrijpen van de AVG-wetgeving en de toepassing ervan op het bedrijf wordt benadrukt.

Het verslag bespreekt ook wie of wat onder de wet valt en hoe het bedrijf moet voldoen aan de regelgeving hiervan, met specifieke aandacht voor de bescherming van de gegevens van kinderen. Het recht op toestemming en het verwijderen van gegevens wordt ook behandeld, evenals de rechten van kinderen onder de wet. Het verzamelen van gegevens binnen de applicatie wordt geanalyseerd, waarbij persoonsgebonden gegevens en niet-persoonsgebonden gegevens worden onderscheiden.

Het onderzoek concludeert dat het bedrijf zich bewust moet zijn van de rechten en verantwoordelijkheden van kinderen onder de AVG en de nodige maatregelen moet nemen om de privacy te waarborgen.

Voorwoord

Voor u licht het onderzoek omtrent de Algemene verordening gegevensbescherming (AVG) binnen Dutch Dolhpins Swimming Club. Het verslag is tot stand gekomen na een goed en uitgebreid onderzoek en analysering van de wet en het bedrijf. Ik heb gekeken naar mogelijke onderzoekmogelijkheden om de AVG-wet zo goed mogelijk te kunnen analyseren en adviseren.

Graag wil ik mijn oprechte dank uitspreken aan Esther Hageraats, die een goede bijdrage heeft geleverd aan het ondersteunen van mij en adviseren voor het onderzoek. Haar expertise en inzichten hebben mij geholpen om de juiste richting te bepalen en belangrijke aspecten goed te specificeren. Zonder haar hulp en betrokkenheid zou dit verslag niet mogelijk zijn geweest.

Ik hoop dat dit onderzoek een waardevolle bijdrage levert aan de bewustzijn en begrip van de bescherming van gegevens binnen het bedrijf. Het is namelijk belangrijk dat de kwetsbare groep kinderen zo goed mogelijk worden beschermd.

Tot slot wil ik alle lezers bedanken voor hun interesse in dit verslag. Ik hoop dat het zal helpen om een beter inzicht te krijgen in de gegevensbescherming van de AVG-wet.

Met vriendelijke groet,

Nick beun

Inhoudsopgave

Inleiding

Welkom bij het document AVG onderzoek van projectgroep 3. In dit project gaan we aan de slag met het realiseren van de opdracht die ons is meegegeven in de projectgids voor het zwembad Dutch Dolphins swimming club.

Tijdens dit project is het de bedoeling dat we gaan kijken hoe de wens van de opdrachtgever kan worden gerealiseerd en hoe de applicatie kan worden ontwikkeld die het plezier van leerlingen gaat meten, en tegelijkertijd voldoet aan de AVG-wetgeving.

In dit onderzoek document bestuderen we de regelgeving van de Algemene Verordening Gegevensbescherming (AVG) binnen Nederland en onderzoeken we hoe deze van toepassing is op Stichting Fieldlab Swimming voor het bedrijf Dutch Dolphin Swimming Club. Daarnaast analyseren we de mogelijke gevolgen van gegevensverwerking binnen het ontwerp van een nieuwe applicatie.

Op dit moment heeft het bedrijf baard bij een nieuwe applicatie die tot doel heeft het zwemplezier van kinderen te meten door het gebruik van smileys of dergelijke iconen. Deze iconen zullen uiteindelijk de fundering geven om te kijken welke aspecten kinderen leuk vonden aan de les.

Aangezien de applicatie gegevens van kinderen verwerkt en hierbij persoonlijk identificeerbare informatie betreft, is het van groot belang om rekening te houden met de bescherming van deze gegevens. In dit geval komt de wet AVG, ook wel bekend als de General Data Protection Regulation (GDPR) hierbij kijken, dit is een Europese wet die tot doel heeft de privacy en gegevensbescherming van personen te waarborgen. Deze wet is van toepassing op alle organisaties die persoonsgegevens verwerken binnen de Europese Unie, waaronder Nederland.

Voor het bedrijf is het belangrijk dat de gegevens van de applicatie moet voldoen aan de strenge eisen en verplichtingen van de AVG wet. Het gaat hierbij niet alleen om het verzamelen en verwerken van persoonsgegevens, maar ook om de beveiliging en bescherming ervan.

Om te voldoen aan de AVG moet er passende en vooral technische maatregelen treffen om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens te waarborgen. Dit omvat het implementeren van beveiligingsmaatregelen, zoals hasing, firewalls en toegangscontrolesystemen, om ongeoorloofde toegang tot de gegevens te voorkomen.

Bovendien moeten er strikte procedures worden gevolgd bij de verwerking van persoonsgegevens, inclusief het verkrijgen van de juiste toestemming van de ouders of wettelijke voogden van de kinderen. Het bedrijf moet ook zorgen voor transparantie en duidelijkheid over welke gegevens worden verzameld, hoe deze worden gebruikt en met wie ze worden gedeeld.

1. Begrippenlijst

In dit hoofdstuk zullen we gaan kijken naar wat alle gebruikte begrippen zijn in dit onderzoeksverslag. Hier wordt genoteerd wat de betekenis is van een bepaald begrip en hoe dit specifiek wordt bedoeld in het onderzoeksverslag

- **AV**
  Algemene Verordening Gegevensbescherming. Ook bekend als GDPR (General Data Protection Regulation), is een Europese wet die de privacy en gegevensbescherming van personen waarborgt. AVG is de Nederlandse wet.
- **GDPR**
  General Data Protection Regulation. Zie bovenstaand in de Begrippenlijst
- **Firewall(s)**
  Beveiligingsmaatregelen die worden gebruikt om ongeautoriseerde toegang tot een netwerk of computersysteem te voorkomen. Ze controleren het inkomende en uitgaande netwerkverkeer op basis van vooraf ingestelde regels.
- **Pseudonimisering**
  Een techniek waarbij persoonlijke gegevens worden vervangen door pseudoniemen, waardoor de identificatie van personen moeilijker wordt zonder het gebruik van aanvullende informatie. Het is een vorm van gegevensverwerking die de privacy van personen beschermt.
- **Autoriteit Persoonsgegevens**
  De Nederlandse toezichthoudende autoriteit voor de naleving van de AVG. Het is verantwoordelijk voor het toezicht houden op de verwerking van persoonsgegevens en het handhaven van de privacy rechten van personen.
- **Anonimiseren/Anonimisering**
  Een proces waarbij persoonlijke gegevens zodanig worden gewijzigd of verwijderd dat de identiteit van een persoon niet langer kan worden achterhaald. Anonieme gegevens zijn niet langer herleidbaar tot een specifiek individu.
- **Beveiliging audits**
  Een proces waarbij de beveiligingsmaatregelen van een organisatie worden geëvalueerd en getest om mogelijke kwetsbaarheden en risico's te identificeren. Het omvat het beoordelen van beveiligingsprotocollen, systemen en processen om de effectiviteit ervan te waarborgen.
- **Gegevensverwerker**
  Een organisatie of persoon die persoonsgegevens namens een verwerkingsverantwoordelijke verwerkt.
- **Gegevensbeschermingseffectbeoordeling**
  Dit is een controle om te zien of er problemen zijn met het verzamelen en gebruiken van persoonlijke gegevens. We willen ervoor zorgen dat de privacy goed wordt beschermd. We kijken naar welke gegevens we hebben, wat we ermee doen en met wie we ze delen. Daarna nemen we maatregelen om problemen te voorkomen en de gegevens veilig te houden.
- **Datalek**
  Een datalek is een incident waarbij ongeoorloofde toegang, verlies, diefstal of onbedoelde openbaarmaking van persoonsgegevens plaatsvindt.
- **Toestemming**
  Toestemming vereist naar goedkeuring die een person verleent voor de verwerking van zijn of haar persoonsgegevens.
- **Applicatie**
  De applicatie verwijst naar de ontworpen applicatie van de software engineers binnen het

project. Zie meer informatie over wat en hoe de applicatie werkt hier: Gegevens van de applicatie.

- **AVG-Vriendelijk**
  Verwijst naar iets dat in overeenstemming is met de AVG wet.
- **Vernietigd**
  Dit wordt gezien als het verwijderen en opruimen van alle destijds gebruikte gegevens die niet op een veilige wijze zijn opgeslagen.
- **Kwaadwillende**
  Dit houdt in dat er personen de intentie hebben om opzettelijk schade willen brengen.
- **Benodigde doel**
  Hiermee wordt bedoeld dat verzamelde gegevens alleen worden gebruikt voor het daadwerkelijke verzameldoel.

2. Onderzoeksmogelijkheden

Om dit onderzoek succesvol te kunnen starten moeten we gaan kijken hoe we het onderzoek tot succes kunnen brengen, hiervoor kunnen we verschillende onderzoekmethodes voor gaan gebruiken.

Er zijn verschillende onderzoeksmogelijkheden om dit onderzoek tot stand te kunnen brengen, onderstaand heb ik een kleine lijst verzameld met onderzoeksmogelijkheden die relevant kunnen zijn om te gebruiken, dit onderstaande methodes worden gebruikt in dit verslag:

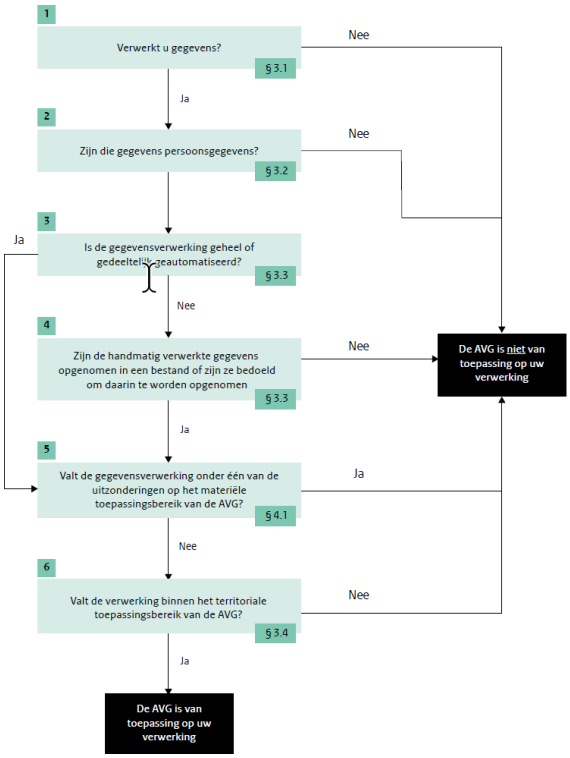
- **Literatuurstudie**
  Een studie van relevante literatuur, wet- en regelgeving, en bestaand onderzoek met betrekking tot de AVG en gegevensbescherming. Dit kan helpen bij het verkrijgen van een goed begrip van de regelgeving, richtlijnen en best practices met betrekking tot gegevensbescherming, met name bij de verwerking van persoonsgegevens van kinderen.
- **Requirements Analyse**
  Een requirements analyse is een aanpak om de behoeften en doelen van een systeem te identificeren en vast te leggen. Het houdt ook wel in dat het verzamelen en documenteren van functionele en niet functionele vereisten, ook wel requirements genoemd. Als doel voor dit document is het dan ook om een dieper inzicht te krijgen in wat het systeem moet doen om de realisatie te kunnen volbrengen. Ook wel de basis voor het uiteindelijke ontwerp

Voor het onderzoek is het van belang dat we gebruik gaan maken van literatuurstudie, hierbij gaan we ons verdiepen in de AVG-wetgeving en een uitstekende analyse maken.

3. Valt het bedrijf onder de AVG-wet?

Het is natuurlijk als bedrijf van belang om erachter te komen of je onder de AVG-wet valt en of deze voor jou als bedrijf strikt van toepassing is, voor de AVG-wet kan dit wel of niet van toepassing zijn op de gegevensverwerking binnen je bedrijf. Na het erbij pakken van de handleiding van (Schermer & Toornstra, 2023) biedt een goede opzet van de AVG wet.

Binnen in dit document wordt genoteerd of je wel of niet moet verwachten of AVG van toepassing is op je verwerking. Daarom is het belangrijk dat er als eerst moet worden gekeken of het bedrijf sprake heeft van een AVG wetgeving, of dergelijke. Hiervoor gebruiken we de onderstaande afbeelding die is meegeleverd door de Rijksoverheid (Schermer & Toornstra, 2023), deze afbeelding toont heel eenvoudig wanneer er sprake is van naleving van de AVG wet.



Figuur 1- Afbeelding van Rijksoverheid.nl

Tijdens de ontwikkeling van de applicatie komen er verschillende gebruikersgegevens naar voren, die geclassificeerd zijn als gebruikers gegevens. Deze gegevens worden automatisch gebruikt in de applicatie en valt op de materiele toepassingsbereik van de AVG. Hierdoor is het bedrijf direct verantwoordelijk voor het verwerken van gegevens.

Om te kunnen zorgen dat het bedrijf voldoet aan alle AVG regelgevingen moet er zorgvuldig worden gekeken wat de beveiligingsopties kunnen zijn en hoe het bedrijf in de toekomst et deze regelgeving om kan gaan. Binnen dit document worden alle rechten van kinderen uitgelegd en worden verschillende toekomstige uitgekaard.

3.1 Richtlijnen van de AVG-Wet

In dit onderdeel wordt een grondige analyse van de AVG-richtlijnen met betrekking tot gegevensbescherming, gegevensverwerking en privacy rechten gedaan. Hierbij kan onderzocht worden welke specifieke bepalingen van toepassing zijn op het verwerken van persoonsgegevens van kinderen en hoe het bedrijf aan deze bepalingen moet voldoen.

Volgens de AVG wet in Nederland worden kinderen beschouwd als kwetsbare personen, “Artikel 8 AVG | Overweging 38 (voorwaarden voor toestemming van kinderen bij het gebruik van diensten van de informatiemaatschappij)” (Schermer & Toornstra, 2023, p. 39) deze groep kwetsbare personen verdient speciale aandacht tot betrekking van hen persoonsgegevens.

Om tot de AVG te voldoen bij het verwerken van persoonsgegevens van kinderen moet het bedrijf verschillende maatregelingen nemen. Er moet toestemming worden gevraagd omtrent het gebruik van gegevens, er moet dus duidelijke en begrijpelijke toestemming wordt verkregen, dit moet worden gevraagd aan de ouders of wettelijke vertegenwoordigers van het kind, voordat deze gegevens worden verwerkt of worden gebruikt.

3.1.1 Toestemming en verwijderrecht

Toestemming en het recht op het verwijderen van gegevens zijn belangrijke onderdelen van de gegevensbescherming, vooral als het om de persoonsgegevens gaat van kinderen. In een geval als dit is het belangrijk dat er wordt gezorgd dat ouderen het zeggenschap hebben over welke gegevens van hun kinderen er worden gedeeld en dat er actie wordt ondernomen om de privacy van kinderen te waarborgen.

Bij het zwembad wordt er gebruik gemaakt van de voornamen van kinderen deze worden gebruikt zodat kinderen weten wie ze zijn en welk profiel van hen is in de nieuw ontwikkelde applicatie. Aangezien een voornaam herleidbaar is naar een persoon wordt dit als gevoelige gegevens gezien, er moet ten alle tijden toestemming worden gevraagd wanneer de gegevens van een kind wordt verzameld. Een ouder moet begrijpen waar hen gegevens voor worden gebruikt en wat het doel is van deze gegevens.

Indien een ouder of wettelijk aangewezen voogd wenst dat gegevens worden verwijderd, kunnen deze worden geanonimiseerd. Hierbij kunnen we gebruik maken van pseudonimisering -/of anonimiseren, waarbij persoonlijke gegevens worden vervangen, zoals de voornaam van het kind. In plaats van een voornaam wordt dan een unieke reeks van cijfers en/of nummers gebruikt om het kind te identificeren. Op deze manier kunnen de gegevens blijven bestaan, zodat het zwembad ook nadat het kind is gestopt met zwemmen kan kijken naar de resultaten, zonder dat er inbreuk wordt gemaakt op de rechten van het kind.

Ouders moeten waar nodig gegevens op kunnen vragen van zijn of haar zoon -/of dochter en hebben het recht om deze gegevens te laten verwijderen, of ook wel eerder benoemd pseudonimiseren -/of anonimiseren (Schermer & Toornstra, 2023, p. 14).

Op basis van het hoofdstuk 7 in de AVG wet (Schermer & Toornstra, 2023) staat welke rechten betrokkenen hebben en of je gehoor aan deze rechten hoort te geven. Ook staat hier de gemiddelde reageertijd en hoelang je er gemiddeld over mag doen.

3.1.2 Rechten van kinderen

Volgens de AVG-wet hebben kinderen ook specifieke rechten en verantwoordelijkheden met betrekking tot het verwijderen van hun eigen gegevens, bijvoorbeeld bij een zwembad. Een kind heeft het recht om een verzoek in te dienen om zijn of haar gegevens te laten verwijderen. Het is echter belangrijk om te benadrukken dat volgens de Rijksoverheid "wanneer toestemming wordt gevraagd in het kader van diensten van de informatiemaatschappij (bijvoorbeeld online winkels en sociale media) en de persoon is jonger dan zestien jaar, dan moeten de ouders of voogden toestemming geven" (Schermer & Toornstra, 2023, p. 39).

Dit betekent dat kinderen van 16 jaar of ouder kunnen verzoeken om hun gegevens te laten verwijderen, op voorwaarde dat er geen wettelijke verplichtingen zijn die het zwembad tegenhouden om deze gegevens te verwijderen. Bovendien is het belangrijk om te benadrukken dat zelfs als er al toestemming is gegeven voor het gebruik van de gegevens, deze toestemming op elk moment kan worden ingetrokken. Het kind behoudt het recht om zijn of haar toestemming in te trekken, waarna het zwembad verplicht is om de gegevens te verwijderen.

Het is van groot belang dat Dutch Dolphins zich bewust is van de rechten en verantwoordelijkheden van kinderen die vallen onder de AVG-wet en de nodige maatregelen neemt om deze rechten te respecteren. Dit omvat het faciliteren van het verwijderen van persoonsgegevens wanneer een kind hierom vraagt, in overeenstemming met de geldende wettelijke bepalingen. Het zwembad moet het verzoek accepteren en binnen een redelijke termijn reageren. Er wordt normaliter verwacht dat dit binnen een maand gebeurt (yoursafetynet.com, n.d.).

Er dient ook rekening gehouden te worden met het feit dat gegevens van kinderen als extra gevoelig worden beschouwd. Zelfs als het kind inmiddels volwassen is en destijds toestemming heeft gegeven, moet dit serieus genomen worden. Destijds was de persoon namelijk niet op de hoogte van de mogelijke risico's (Schermer & Toornstra, 2023, p. 81).

3.2 Toelichting van de applicatie

Deze sectie gaat over de ontwikkeling van de software, die in dit onderzoeksverslag ook wel "applicatie" genoemd, zie Begrippenlijst. Het ontwikkelproces wordt uitgevoerd door softwareontwikkelaars van het projectgroep, en is gericht op het voldoen aan de wensen en eisen van de opdrachtgever, Dutch Dolphins swimming club.

Het doel van de applicatie is om het verzamelen van gegevens voor het bedrijf te vergemakkelijken. Een gedetailleerde beschrijving van de behoeften en wensen van de opdrachtgever is te vinden in Figuur 5 - Bijlage 1, de opdrachtomschrijving.

De ontwikkeling van de applicatie is gericht op het vervullen van de wensen van de opdrachtgever. Een van deze wensen is het vermogen van de applicatie om het plezier van de leerlingen te meten met behulp van een beoordelingssysteem. Het beoordelingssysteem zorgt ervoor dat alleen geauthentiseerde accounts, ook wel leraren genoemd, toegang hebben tot de beoordelingen. Meer informatie over de gegevens die kunnen worden bekeken door geauthentiseerde gebruikers is te vinden bij kop “Gegevens van docenten (account)”.

Door de ontwikkeling van deze applicatie hoopt de opdrachtgever een gebruiksvriendelijke en effectieve oplossing te krijgen om gegevens te verzamelen en het plezier van leerlingen te meten.

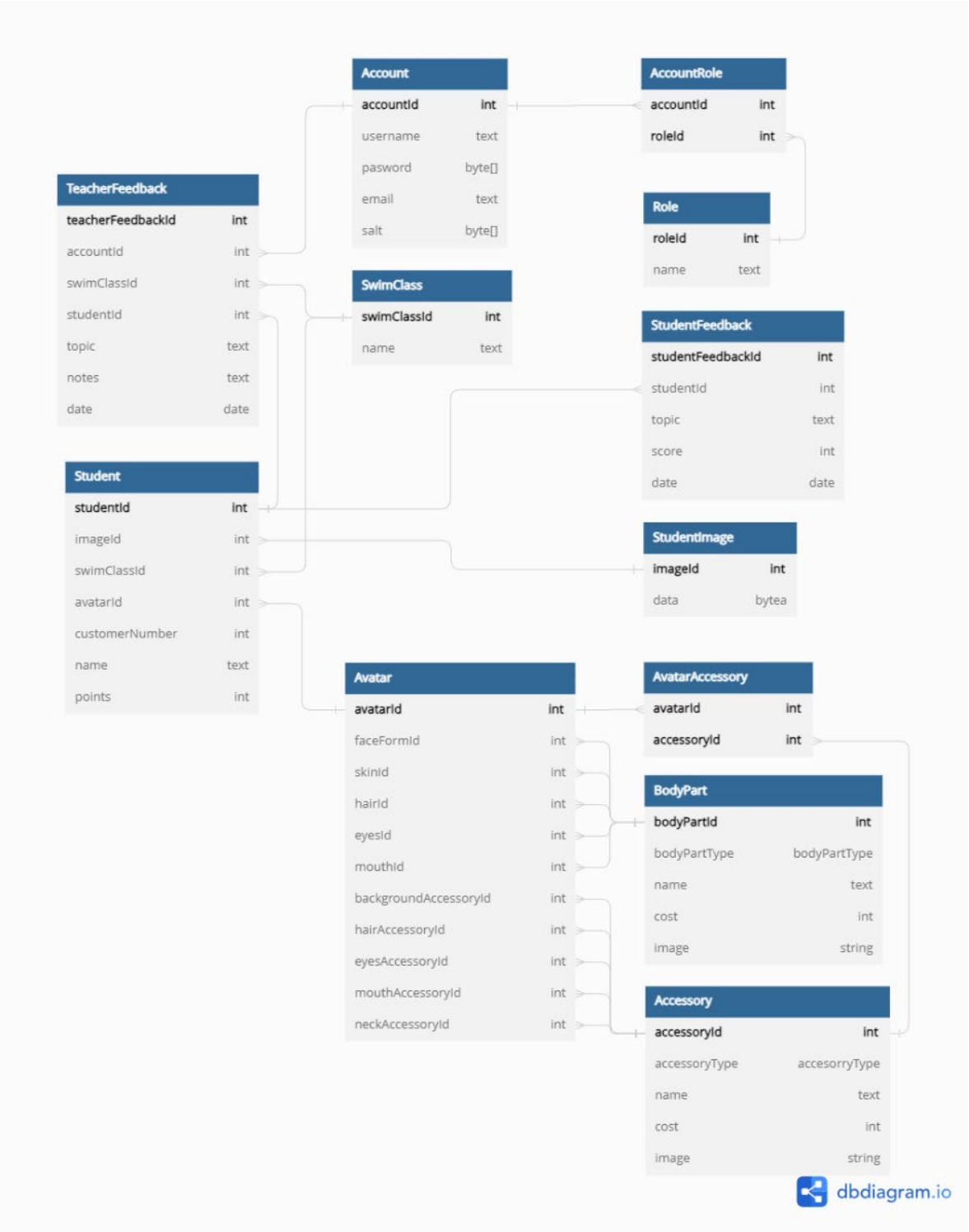
3.2.1 Gegevensverwerking van de applicatie

In dit hoofdstuk moet worden gekeken welke gegevens er op dit moment worden verzameld binnen de applicatie om zo’n duidelijk mogelijke blik te krijgen welke gegevens gevoelig zijn. Om dit te kunnen doen moeten we gaan kijken wat de verschillende soorten persoonsgegevens zijn die op dit moment worden verzameld en waar nodig verwerkt binnen in de nieuw ontworpen applicatie van het bedrijf.

Het is cruciaal om te weten welke gegevens als gevoelig worden geclassificeerd, dit maakt het dan uiteindelijk mogelijk om de juiste beveiligingen toe te passen om de privacy van de personen zoveel mogelijk te kunnen waarborgen.

Tijdens de ontwikkeling van de applicatie hebben we een database diagram opgesteld om te gaan kijken welke gegevens er worden verzameld, hoe deze gegevens aan andere onderdelen van de applicatie moeten worden ingesteld en hoe de database zo fijn en overzichtelijk mogelijk kan worden ingedeeld.

In het onderstaande ontwerp is zichtbaar waar alle gegevens aan gelinkt zijn en hoe deze binnen in de applicatie worden gestuurd:



Figuur 2 - Database indeling voor de applicatie

Nu we het bovenstaande ontwerp weten, gaan we kijken wat de gegevens die hier staan nu specifiek betekenen en hoe deze worden verwerkt met betrekking tot de gevoeligheid van de persoonsgegevens. Dit wordt in hoofdstuk 3.2.2 beter toegelicht.

3.2.2 Gegevens toelichten

Om erachter te kunnen komen welke gegevens persoonsgebonden zijn en welke dat niet zijn wordt er in de tabellen gebruik gemaakt van een specifieke classificatie, deze wordt hieronder toegelicht:

1. **Persoonsgebonden gegevens:**
   Dit omvat informatie zoals naam, geboortedatum, contactgegevens, adres, en andere gegevens die direct naar een specifiek individu kunnen leiden. Het is van essentieel belang om bij het verzamelen en verwerken van dergelijke gegevens te zorgen voor de juiste beveiligingsmaatregelen en naleving van de AVG-regelgeving.

2. **Niet-persoonsgebonden gegevens:**
   Dit omvat gegevens die op zichzelf niet kunnen leiden tot identificatie van een persoon. Voorbeelden hiervan zijn geanonimiseerde gebruiksstatistieken, geaggregeerde gegevens over zwemplezier of andere niet-identificeerbare informatie. Hoewel deze gegevens op zichzelf niet gevoelig zijn, is het toch belangrijk om passende maatregelen te nemen om de privacy van gebruikers te waarborgen en te voorkomen dat deze gegevens worden herleid tot een persoon.

3. **Gevoelige gegevens:**
   Dit omvat informatie die als bijzonder gevoelig wordt beschouwd, zoals gezondheidsgegevens, prestatiegegevens of andere persoonlijke details die een verhoogd risico op misbruik met zich meebrengen.

   Het is van cruciaal belang om uiterst voorzichtig om te gaan met dergelijke gegevens en ervoor te zorgen dat ze alleen worden verzameld en verwerkt indien absoluut noodzakelijk, met de juiste juridische basis en toestemming van betrokkenen (Schermer & Toornstra, 2023, p. 24).

Onderstaand staan twee tabellen die meer informatie geven over de gegevensgevoeligheid:

3.2.2.1 Gegevens van kinderen (student)

Onderstaand is zichtbaar welke gegevens op dit moment zichtbaar zijn binnen de applicatie, ook is zichtbaar of deze eventueel herleidbaar zijn.

Gegevens	Persoonsgebonden	Gevoelig	Beveiliging
name	Ja	Nee	Belangrijk
customernumber	Nee	Nee	Niet van belang
avatarid	Nee	Nee	Niet van toepassing
studentfeedbackid	Misschien	Nee	Zou fijn zijn
notes	Ja	Nee	Belangrijk
swimmclassid	Ja	Nee	Zou fijn zijn

Tabel 1 - Gegevens van (student)

3.2.2.2 Gegevens van docenten (account)

Onderstaand is zichtbaar welke gegevens op dit moment zichtbaar zijn binnen de applicatie, ook is zichtbaar of deze eventueel herleidbaar zijn.

Gegevens	Persoonsgebonden	Gevoelig	Beveiliging
email	Ja	Ja	Belangrijk
username	Ja	Nee	Niet van toepassing
password	Ja	Ja	Belangrijk

Tabel 2 - Gegevens van (account)

3.2.3 Waar komt de gegevenstoevoer vandaan

De gegevens die worden opgeslagen in de nieuwe applicatie staan gespecificeerd in Figuur 2 - Database indeling voor de applicatie.

De opdrachtgever Dutch Dolphins die baart heeft bij de ontwikkeling van de nieuwe applicatie heeft momenteel al een groot aantal gegevens die volgens de AVG worden opgeslagen.

De gegevens die momenteel beschikbaar zijn voor het bedrijf worden momenteel gebruikt bij een applicatie binnen het zwembad, het bedrijf wilt geen specifieke informatie delen over deze applicatie of gebruikswijze hiervan. Echter geeft het bedrijf wel aan dat de gegevens die momenteel worden gebruikt AVG-vriendelijk zijn.

Omdat het bedrijf op het moment al bestaande gegevens heeft, heeft het baart bij een gegevensexport van de bestaande gegevens naar de nieuwe applicatie. Dit kan worden gedaan met behulp van een Excel bestand, het is echter wel de verantwoordelijkheid van het bedrijf om AVG-vriendelijk mee om te gaan. Hiervoor wordt dan ook mee bedoeld dat het Excel bestand als vertrouwelijk wordt gezien en dat wanneer de plicht is voltooid dat de gegevens worden vernietigd.

3.3 Gegevensverwerking en doelen

In dit onderdeel wordt gekeken naar de specifieke manieren waarop de verzamelde gegevens worden verwerkt binnen het applicatieontwerp. Hierbij kan gekeken worden naar de technische processen en procedures die worden gebruikt om de gegevens te verzamelen, op te slaan, te analyseren en te gebruiken voor het meten van zwemplezier van kinderen.

Binnen de applicatie die wordt ontworpen voor het zwembedrijf moet worden gekeken hoe gegevens worden verwerkt, waar deze naar toe worden verstuurd en waar de gegevens van kinderen worden gebruikt. In het geval van het zwembedrijf wordt er verwezen naar het verzamelen, opslaan, gebruik van de persoonsgegevens.

3.3.1 Doelen specificatie

In dit onderdeel staan de doelen beschreven op basis van de vorige teksten uit Toestemming en verwijderrecht, Rechten van kinderen en Gegevens toelichten. Deze doelen worden in Definiëren van de doelen geanalyseerd, sommige doelen worden later in de tekst behandeld.

1. Het doel om een efficiënt en veilig proces op te zetten voor de verzameling van gegevens.
2. Het doel om een procedure te vinden die gegevens veilig op te slaan en te beschermen.
3. Het doel om te zorgen dat gegevens alleen voor het benodigde doel (Zie Begrippenlijst) worden gebruikt.
4. Het doel om transparantie te bieden aan ouders en verzorgers.

3.3.2 Definiëren van de doelen

Zoals hierboven beschreven heeft het zwembedrijf baat bij het verzamelen, opslaan en gebruik van persoonsgegevens. Laten we nu kijken naar de specifieke doelen en hoe deze worden gebruikt.

Bij het verzamelen van gegevens worden er gegevens verzameld over de ervaringen van de kinderen tijdens de zwemlessen. Na elke zwemles heeft het kind de mogelijkheid om binnen de applicatie op zijn of haar profiel te klikken en een beoordeling te geven over hoe hij of zij de zwemles heeft ervaren.

Het doel van gegevensverwerking is dus om waardevolle informatie te verzamelen over het plezier en de tevredenheid van kinderen tijdens de zwemlessen. Deze informatie kan het zwembad ondersteunen bij het identificeren van kwaliteitsproblemen of verbeteringen in het lesprogramma. Met behulp van de beoordelingen van kinderen krijgen zweminstructeurs een specifiek overzicht van de onderdelen die verbeterd kunnen worden. Ze kunnen specifieke vragen stellen waarop kinderen een beoordeling kunnen geven.

Het is belangrijk op te merken dat bij deze gegevensverwerking de privacy van de kinderen gerespecteerd moet worden en dat de nodige maatregelen moeten worden genomen om de gegevens veilig en vertrouwelijk te behandelen. Toestemming van de ouders moet worden verkregen voordat persoonsgegevens van kinderen worden verzameld en verwerkt, zoals vereist word. Nadat de gegevens zijn verzameld en verwerkt, is het belangrijk om te begrijpen hoe deze gegevens worden gebruikt binnen het de applicatie voor het zwembedrijf.

Met de verzamelde gegevens over de ervaringen van kinderen tijdens de zwemlessen kan het zwembedrijf waardevolle inzichten verkrijgen. Deze inzichten kunnen worden gebruikt om de kwaliteit van de lessen te verbeteren, problemen aan te pakken en de algehele tevredenheid van de kinderen te vergroten.

3.4 Toestemmingsverplichting

In dit onderdeel wordt onderzoek gedaan naar de toestemmingsvereisten volgens de AVG, met name met betrekking tot de verwerking van persoonsgegevens van kinderen. Het omvat het onderzoeken van de vereisten voor het verkrijgen van toestemming van ouders of wettelijke voogden en hoe het bedrijf dit proces adequaat kan implementeren.

Volgens de AVG is altijd toestemming vereist van ouders of wettelijke voogden voor de verwerking van persoonsgegevens van kinderen, met name bij het gebruik van een applicatie, zoals die mogelijk door het zwembad wordt gebruikt. De manier waarop toestemming wordt gevraagd kan variëren, maar over het geheel genomen moeten ouders goed geïnformeerd zijn over het systeem dat wordt gebruikt. Ook moet duidelijk zijn wat er met deze gegevens gebeurt en moet er op een duidelijke en eenvoudige manier worden uitgelegd hoe dit wordt gedeeld. Op die manier kunnen ouders gemakkelijk beslissen of ze al dan niet toestemming willen geven.

Het ontwikkelingsteam van de applicatie moet ervoor zorgen dat ouders op een eenvoudige en effectieve manier toestemming kunnen geven voor de verwerking van de gegevens van hun kinderen. Dit betekent dat er geen vooraf aangevinkte vakjes of "stilzwijgende" toestemming mogen worden gebruikt. Alle vakjes moeten leeg zijn voordat ze worden gebruikt en mogen niet vooraf worden ingevuld. Naast het gebruik van een vakje kan ook een fysiek of digitaal toestemmingsformulier worden gebruikt.

Het zwembad moet ook zorgen voor een eenvoudige manier waarop ouders hun toestemming kunnen intrekken als ze dat willen. Ouders hebben te allen tijde het recht om de gegeven toestemming in te trekken. Het zwembad moet ervoor zorgen dat dit intrekkingsproces net zo eenvoudig is als het geven van toestemming.

Wanneer een ouder of wettelijke voogd toestemming heeft gegeven, moet er een register of opslagplaats worden bijgehouden van de verwerkingsactiviteiten die plaatsvinden met de gegevens van de kinderen. Dit is een verplichting wanneer er gebruik wordt gemaakt van deze gegevens of wanneer er recht is om deze gegevens te gebruiken en/of te verwerken.

3.5 Beveiligingsmaatregelingen

In dit onderdeel wordt er een evaluatie van de huidige beveiligingsmaatregelen binnen het applicatieontwerp om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens te waarborgen. Dit kan het onderzoeken van versleutelingstechnieken, toegangscontroles, auditsporen en andere beveiligingspraktijken omvatten.

Tijdens het ontwerpen van de systemen moet er zorgvuldig worden nagedacht over de verschillende beveiligingswijzes om te zorgen dat de systemen veilig en zo goed mogelijk functioneren. De onderstaande lijst laat zien welke beveiligingsmaatregelingen moeten worden overwogen:

1. **Versleuteling**
   Er moet worden gezorgd voor het versleutelen van de gegevens die worden verzameld en verwerkt. Versleuteling zorgt ervoor dat de gegevens onleesbaar zijn voor onbevoegden, zelfs als ze toegang krijgen tot de gegevens. Een versleuteling als de AES-256 zou een geschikte methode zijn om te zorgen dat de gegevens goed beveiligd zijn.

2. **Firewall(s)**
   Er moeten firewalls worden geïmplementeerd om ongeautoriseerde toegang tot het netwerk en het computersysteem te voorkomen. Firewalls controleren het inkomende en uitgaande netwerkverkeer en blokkeren of filteren verdachte activiteiten.

3. **Toegangscontrolesystemen**
   Er moet een toegangscontrolesysteem worden geïmplementeerd om te zorgen voor geautoriseerde toegang tot de gegevens. Dit kan bijvoorbeeld worden bereikt door het gebruik van sterke wachtwoorden die worden beveiligd met een hashfunctie of dergelijke encryptiemethode. Een functie als tweefactor authenticatie zou mooi zijn meegenomen en het beperken van de toegang tot alleen personeel dat het daadwerkelijk nodig hebben.

4. **Toestemmingsprocedure(s)**
   Er moet een strikte procedures volgen bij het verkrijgen van toestemming van ouders of wettelijke voogden voor het verzamelen en verwerken van persoonsgegevens van kinderen. Dit omvat het verkrijgen van duidelijke en begrijpelijke toestemming en het zorgen voor transparantie over het gebruik van de gegevens.

5. **Beveiligingsaudits**
   Er moeten regelmatig beveiligingsaudits worden uitgevoerd om mogelijke kwetsbaarheden en risico's te identificeren. Dit omvat het beoordelen van beveiligingsprotocollen, systemen en processen om ervoor te zorgen dat ze effectief zijn en aan de vereisten van de AVG voldoen.

6. **Pseudonimisering**
   Het is mogelijk dat er gebruik wordt gemaakt van pseudonimisering om de identificatie van personen moeilijker te maken zonder het gebruik van aanvullende informatie. Dit kan bijdragen aan het beschermen van de privacy van kinderen.

7. **Verwijderrecht**
   Het bedrijf moet voldoen aan het recht van ouders en kinderen om gegevens te laten verwijderen of te laten pseudonimiseren, indien gewenst. Dit omvat het ontwikkelen van procedures en systemen om aan dergelijke verzoeken te voldoen binnen de gestelde termijnen.

3.6 Datalekken en meldingsplicht

In dit onderdeel wordt onderzoek gedaan naar de vereisten en procedures voor het melden van datalekken volgens de AVG. Er wordt gekeken naar de maatregelen die het bedrijf moet nemen om datalekken te voorkomen, detecteren en melden aan de juiste autoriteiten en betrokkenen volgens de Algemene Verordening Gegevensbescherming (AVG) in Nederland. Deze wet legt strikte regels en vereisten op voor de bescherming van persoonsgegevens en benadrukt de verantwoordelijkheid van organisaties om datalekken te voorkomen en tijdig te reageren op dergelijke lekken.

Om datalekken te voorkomen, moet het zwembad passende maatregelen nemen, zoals het implementeren van veiligheidsmaatregelen (bijv. gegevensversleuteling), beperkte toegangsrechten tot persoonsgegevens en regelmatige beveiligingsaudits. Het is ook cruciaal dat alle medewerkers die toegang hebben tot persoonsgegevens op de hoogte zijn van de privacy procedures en de mogelijke gevolgen van datalekken, eventueel zou het verstandig zijn om medewerkers hier op te laten trainen.

3.6.1 Tijd voor meldplicht

Het zwembad is verplicht om een datalek onverwijld te melden aan de Autoriteit Persoonsgegevens.

De melding moet altijd binnen 72 uur na ontdekking van het datalek plaatsvinden (Schermer & Toornstra, 2023, p. 65), tenzij het geen risico vormt voor de rechten van de betrokkenen. De melding aan de Autoriteit Persoonsgegevens moet informatie bevatten over de aard en omvang van het datalek, evenals de genomen maatregelen om het datalek aan te pakken en toekomstige inbreuken te voorkomen.

Naast de melding aan de Autoriteit Persoonsgegevens kan het zwembad ook verplicht zijn om betrokkenen op de hoogte te stellen van het datalek, vooral als het lek een hoog risico vormt voor hun rechten en vrijheden. Het zwembad moet de getroffen gebruikers informeren over de aard van het datalek, de mogelijke gevolgen en de maatregelen die zij kunnen nemen om hun persoonsgegevens te beschermen.

Het bedrijf moet te allen tijde op de hoogte blijven van de vereisten en procedures voor het melden van datalekken. Nu we weten hoe de meldplicht werkt, moeten we kijken naar de specifieke stappen die het bedrijf moet nemen om een melding te maken.

1. **Onmiddellijke actie:**
   Bij ontdekking van een datalek moet het zwembad onmiddellijk actie ondernemen om de schade zoveel mogelijk te beperken. Dit kan onder andere inhouden dat de getroffen systemen worden afgesloten en de oorzaak van het lek wordt geïdentificeerd. Er moeten maatregelen worden genomen om een dergelijke situatie in de toekomst te voorkomen.

2. **Melding aan de Autoriteit Persoonsgegevens:**
   Het bedrijf is verplicht om binnen 72 uur na ontdekking van het lek een melding te doen bij de Autoriteit Persoonsgegevens (Schermer & Toornstra, 2023, p. 65). De melding moet informatie bevatten over de aard van het datalek, de mogelijke gevolgen en de genomen maatregelen.

3. **Communicatie met betrokkenen:**
   Als het datalek een hoog risico vormt voor de rechten en vrijheden van betrokkenen, moet het zwembad hen op de hoogte stellen. Dit omvat het informeren van de getroffen

gebruikers over de aard van het datalek, de mogelijke gevolgen en de maatregelen die zij kunnen nemen om hun persoonsgegevens te beschermen.

3.6.2 Gevolgen

Nu het duidelijk is over de meldplicht en wat de eventuele vervolgstappen zijn moeten we specifieker gaan kijken naar de gevolgen die na zich voordoen na het data lek met betrekking tot de AVG-wet.

Het is natuurlijk altijd mogelijk dat een datalek voorkomt, maar het zwembedrijf zal er ten alle tijden voor moeten zorgen dat dit wordt voorkomen. De hoogte van de boetes kunnen namelijk heel erg variëren, afhankelijk van de ernst van het lek dat is veroorzaakt en de mogelijke omstandigheden van de overtreding. De boetes voor eventuele kleine overtredingen waarbij de ernst beperkt is hebben vaak lagere boetes. Wanneer het datalek ernstig is of er is sprake van een herhaaldelijke overtreding dan is het mogelijk dat de boete vele malen hoger zijn. Om een beter beeld te krijgen zijn dit de maximale boetes die kunnen worden opgelegd:

- “Overtredingen van de bepalingen die zien op de (verantwoording(s))plichten die rusten op organisaties, zoals het doen van een gegevensbeschermingseffectbeoordeling of het doen van een melding in geval van een datalek, kunnen worden gesanctioneerd met een administratieve boete van maximaal 10 miljoen euro of 2% van de wereldwijde jaaromzet, in het geval deze hoger is.” (Schermer & Toornstra, 2023, p. 94).

- Overtredingen van de bepalingen over de principes, rechtsgrondslagen en rechten van betrokkenen, kunnen worden gesanctioneerd met een administratieve boete van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet, in het geval deze hoger is. (Schermer & Toornstra, 2023, p. 94).

Wanneer er een boete wordt opgelegd heeft de Autoriteit Persoonsgegevens het recht de boete te laten bepalen met bepaalde factoren zoals de ernstigheid van de overtreding en hoe lang het heeft geduurd tot het lek is gedicht (ook wel de duur van de overtreding). De boete kan ook worden bepaald door de getroffen maatregel om de schade te beperken en te herstellen en het soort persoonsgegevens die getroffen zijn binnen het datalek.

3.7 Requirements

Voor dit hoofdstuk gaan we kijken wat de requirements zijn die uit de bovenstaande tekst is gekomen, en wat het nut is van elke requirement. De requirements die hier uit komen zijn infrastructuur gerelateerd om te kijken hoe we de systemen waar de ontworpen applicatie op gaat draaien.

Nu we alle bovenstaande informatie zo specifiek mogelijk hebben uitgelegd gaan we kijken naar de mogelijke requirements die uit het onderzoek zijn gekomen, hiervoor gaan we een tabel opstellen en kijken of deze requirement interessant is voor infrastructuur. Hierna gaan we kijken of deze functioneel of niet-functioneel is.

3.7.1 Requirements voor de infrastructuur

Onderstaand worden requirements opgesteld die belangrijk zijn voor het instellen en opzetten van de infrastructuuromgeving waar de applicatie op gaat draaien.

	Requirement(s)	MoSCoW	F/NF
1	De database moet worden beveiligd met AES-256.	MUST	F
2	Er moeten firewalls aanwezig zijn om data veilig te handelen.	COULD	F
3	Beveiligingsaudits moeten worden uitgevoerd zonder dat er beschadiging is aan het systeem.	MUST	F
4	De applicatie moet voldoen aan de eisen en verplichtingen van de AVG-Wet.	MUST	NF
5	De database moet regelmatig worden geback-upt om gegevensverlies te voorkomen.	MUST	F
6	Een logging-methode om verdachte activiteiten te detecteren om inbreuk te voorkomen.	MUST	F

Tabel 3 – Requirements Infrastructuur

3.7.1.1 Requirements van infrastructuur toegelicht

Nu we alle belangrijke informatie hebben uitgelicht in Tabel 1 – Requirements Infrastructuurs, worden in dit hoofdstuk toegelicht. De requirements die eerder zijn benoemd zijn allemaal op basis van het onderzoek gehaald.

	Infrastructuur requirements toegelicht
1	Dit houdt in dat er een database moet worden aangemaakt in AWS met een AES-256 encryptiemethode. Dit zorgt voor een sterke beveiliging van de opgeslagen gegevens.
2	Dit betekend dat er een firewall moet worden geïmplementeerd om het netwerk te beschermen tegen ongeautoriseerde toegang.
3	Het moet mogelijk zijn dat er beveiligingsaudits worden uitgevoerd, dit houdt in dat deze audits kunnen worden uitgevoerd zonder dat dit de infrastructuur beschadigd.
4	De database moet een back-up mogelijkheid hebben, er moeten regelmatig back-ups worden gemaakt van belangrijke gegevens zodat er geen gegevensverlies is.
5	De ontworpen applicatie moet voldoen aan de AVG-vereisten zoals benoemd is in het AVG onderzoek.
6	De applicatie moet worden voorzien van een manier om te kunnen loggen, dit houdt in dat er een mogelijkheid moet zijn om verdachte activiteiten te kunnen registreren en te monitoren, zo is het mogelijk om kwaadwillende activiteiten te identificeren.

Tabel 4 - Requirements Infrastructuur toegelicht

3.7.2 Requirements voor de software engineers

Onderstaand worden requirements opgesteld die belangrijk zijn voor het instellen en opzetten van de infrastructuuromgeving waar de applicatie op gaat draaien.

	Requirement(s)	MoSCoW	F/NF
1	Er moet een encryptiemethode -/hasing methode aanwezig zijn.	COULD	F
2	Er moet een mogelijk zijn om gegevens op te kunnen vragen.	MUST	F
3	Het moet mogelijk zijn om een gegevens verwijderverzoek te doen.	MUST	F
4	Er moet een toestemmingsverzoek worden verkregen van gebruikers.	MUST	F
5	Er moet een pseudonimisering(s) mogelijkheid zijn.	MUST	F

Tabel 5 - Requirements Software Engineer(s)

3.7.2.1 Requirements van software engineers toegelicht

Nu we alle belangrijke informatie hebben uitgelicht in Tabel 2 - Requirements Software Engineer(s), worden in dit hoofdstuk toegelicht. De requirements die eerder zijn benoemd zijn allemaal op basis van het onderzoek gehaald.

	Software engineer requirements toegelicht
1	Het moet mogelijk zijn dat er gebruik wordt gemaakt van een gegevensversleuteling methode of dergelijke. Een techniek die wordt gebruikt om gegevens onleesbaar te maken.
2	Het moet mogelijk zijn in de applicatie om gegevens op te kunnen vragen die dan met behulp van een Excel bestand in te zien zijn. Kinderen en -/of ouders moeten hier de mogelijkheid tot hebben.
3	De gebruiker moet de mogelijkheid hebben om een gegevensverzoek aan te kunnen vragen, dit kan met behulp van een verzoek indienen richting een e-mail adres zodat de desbetreffende leraar een export kan doen. Echter moet hier wel een duidelijke log van worden gemaakt zodat het herleidbaar is waar en hoe dit is gebeurd.
4	Er moet toestemming worden gevraagd van gebruikers, dit verzoek moet laten zien dat de ouders toestemming geven voor de gegevensverwerking van het kind.
5	Het moet mogelijk zijn wanneer er een gegevensverzoek wordt ingediend dat de gegevens kunnen worden gepseudonimiseerd.

Tabel 6 - Requirements Software Engineer(s) toegelicht

Bibliografie

Schermer, B. W., & Toornstra, J. (2023, April 15). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*, 2.0. (M. v. Veiligheid, Producent) Opgeroepen op Mei 22, 2023, van Handleiding AVG: https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

yoursafetynet.com. (sd). *Wat is recht op vergetelheid*. Opgeroepen op juli 7, 2023, van yoursafetynet.com: https://www.yoursafetynet.com/wat-is-recht-op-vergetelheid/#:~:text=Voor%20de%20verwijdering%20van%20persoonsgegevens,situatie%20de%20betrokkene%20worden%20ingelicht.

Bijlagen

Multidisciplinaire uitvoering door:
1 business IT'er, 4 software engineers en 1 Infrastructuur engineer

2

Project: Maak zwemles leuk!

Klantinformatie

Organisatie:	Stichting Fieldlab Swimming
Naam contactpersoon:	Carlo van der Heijden
E-mailadres:	c.vanderheijden@fieldlabswimming.com
Telefoon:	

Projectinformatie

Beschrijving organisatie:
InnoSportLab de Tongelreep is een top-level zwemlab waar prestaties van topzwemmers geoptimaliseerd worden en waar gewerkt wordt aan de zwemles van de toekomst. De zwemles van de toekomst moet leuker, attractiever en beter zijn dan de zwemles die momenteel aangeboden wordt. Doel is dat uiteindelijk meer kinderen blijven zwemmen na het afronden van de zwemles. De sporter staat centraal en er wordt evidence based gewerkt.

Probleemstelling/context:
Gamification van de zwemles: per jaar starten ca. 190.000 kinderen met zwemles, voor velen van hen is dit de eerste kennismaking met sport en bewegen. Een groot deel van de kinderen vindt de zwemles niet leuk. Wij hebben als doel om de zwemles leuker en beter te maken. We willen dit bereiken door gamification toe te voegen, plezier te meten en door de daadwerkelijke beweegtijd van een kind dat zwemles volgt te verbeteren

Opdrachtformulering:
Voor het meten van plezier hebben we een literatuuronderzoek gedaan, daaruit hebben we een methode gehaald om plezier te meten bij kinderen. Het gaat om feedback in de vorm van 5 smiley's. We kunnen dit al doen door middel van magneetjes op een whiteboard, maar uiteraard is dit geen geschikte manier om resultaten van honderden kinderen per avond te borgen. We zijn dus op zoek naar een geschikte manier om plezier te meten en op een AVG verantwoorde manier op te slaan. Wel moeten resultaten herleidbaar zijn naar het kind het zelf.

Uiteindelijk lijkt een systeem met smileys het meest effectief. We zijn op zoek naar iemand die dit kan vertalen naar een app en bruikbare handelswijze tijdens de zwemles

Figuur 3 - Bijlage 1

Figuur 4 - Bijlage 2