Eindrapport Sarea

Document eigenschappen	
Bestand	Eindrapport Sarea (0.9).docx
Versie	0.9
Datum	20 Januari 2021
Bron	10.2.g
Status	Concept
Vertrouwelijkheid	Vertrouwelijk
Auteur	10.2.e.

INHOUDSOPGAVE

1 DOCUMENTBEHEER

1.1 REVISIES

Datum	Auteur	Versie	Omschrijving
05-01-2021	10.2.e.	0.1	Initieel
19-01-2021	10.2.e.	0.2	Draft
20-01-2021	10.2.e.	0.9	Voor akkoord
	10.2.e.	1.0	Definitief

1.2 GOEDKEURING

Dit document vereist de goedkeuring van de opdrachtgever en opdrachtnemer.

Datum	Auteur	Versie
10.2.e.	Opdrachtgever	1.0
10.2.e.	Project Manager 10.2.g	1.0
10.2.e.	Project Manager Sarea	1.0

1.3 DISTRIBUTIE

Naam	Organisatie	0.1	0.2	0.9	1.0
10.2.e.	10.2.g	●	●	●	●
10.2.e.	10.2.g	●	●	●	●
10.2.e.	10.2.g			●	●
10.2.e.	10.2.g				●
10.2.e.	Politie			●	●

2 INLEIDING

2.1 ACHTERGROND

Er wordt al een aantal jaren gewerkt aan de ontwikkeling van Sarea. Er zijn ontwerp sessies geweest om de mogelijke functionaliteit in kaart te brengen, er is een grafische userinterface ontworpen en er zijn ook al een aantal basiscomponenten ontwikkeld. De ontwerpen en testrapporten zijn goed gedocumenteerd.

Bij het ontwerp van Sarea is met name gelet op de functionele aspecten en minder op de niet-functionele (kwaliteits)eisen, zoals security, privacy, performance en onderhoudbaarheid. Het in kaart brengen van deze kwaliteitseisen, is ook niet goed mogelijk zonder de rollen en verantwoordelijkheden van de stakeholders te concretiseren, zoals het eigenaarschap. Hierdoor ontbreken er een aantal belangrijke functies en is er mogelijk ook een aantal verkeerde keuzes gemaakt in de architectuur. Uit het testrapport blijkt ook dat het huidige platform niet “volwassen” genoeg is om in productie uit te rollen en door te ontwikkelen. Daarnaast worden nog een aantal functionele wensen benoemd die voor de livegang toegevoegd of aangepast dienen te worden.

Om Sarea daadwerkelijk aan een breed publiek beschikbaar te stellen, dient het platform “volwassen” gemaakt te worden.

2.2 DOELSTELLINGEN

Het doel is om het huidige Sarea platform te verbeteren en door te ontwikkelen tot een Prototype, waarbij:

1. De rollen, belangen en verantwoordelijkheden van de stakeholders helder zijn;
2. Het eigenaarschap is geborgd en ingebed binnen een passende administratieve organisatie;
3. Er voldaan wordt aan alle kwaliteitseisen (compliance, governance en de eisen van de diverse stakeholders);
4. Sarea op een betrouwbare omgeving gehost en beheerd kan worden;
5. Alle noodzakelijke functionaliteit aangeboden wordt, het prototype is dus ook een Minimal Viable Product (MVP);
6. Het platform uitgebreid kan worden met nieuwe functionaliteiten en toepassingen zoals data-analyses.

2.3 DOEL VAN DIT DOCUMENT

Todo

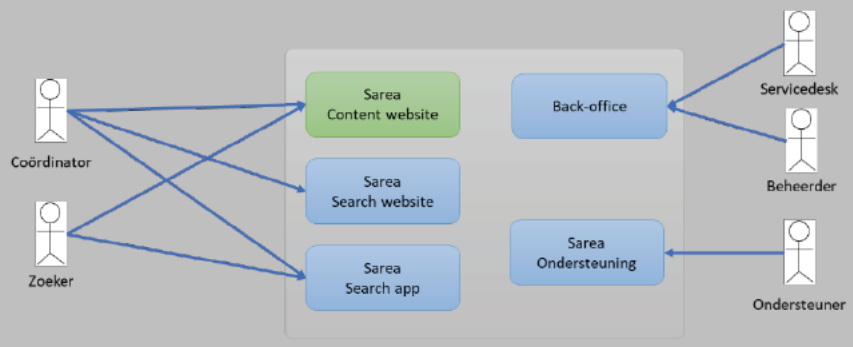
3 INLEIDING

Rollen

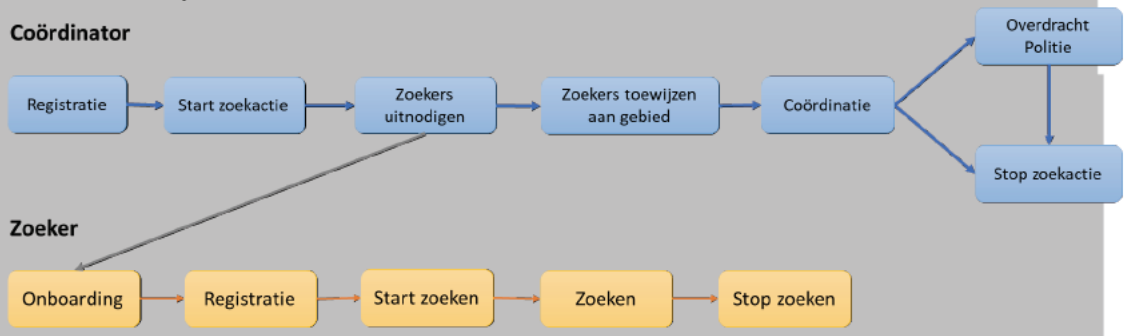
Rol	Toelichting
Bezoeker	Een onbekende gebruiker (dus zonder account)
Zoeker	Een persoon die mee kan gaan zoeken
Coördinator	De coördinator van een zoekactie (mogelijk meerdere per zoekactie)
Politie ondersteuner	Medewerker(s) van de Politie, welke mee kan kijken in de zoekactie
Servicedesk 1e lijns	Beantwoorden van algemene vragen
Servicedesk 2e lijns	Blokkeren van accounts, verwijderen van accounts
Security Officer	Afhandelen van beveiligingsincidenten, bewaken van beveiligingsrisico's
Platform beheerder	Instellen en configureren van het platform, bewaken
Content beheerder	Onderhoud teksten, vertalingen, templates, e-mails

Systemen

Systeem	Toelichting
App	De app die op de smart phone draait
Web - Coördinatorportaal	De website voor coördinatoren
Web - Servicedesk	De website voor de servicedesk
Web - Admin (Back-office)	De website voor de beheer
Web - Ondersteuning	De website voor de ondersteunende partijen zoals Politie



Customer Journey:



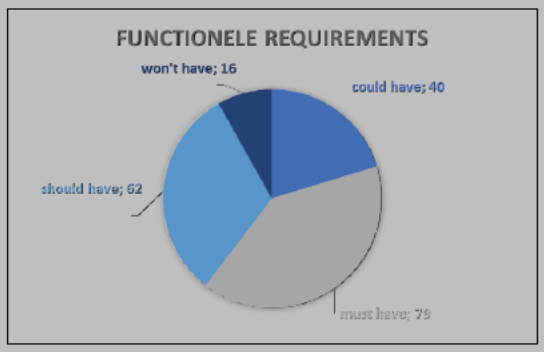
4 FUNCTIONELE EISEN

Op basis van de bestaande documentatie, risk assessment en de interviews met de stakeholders, zijn 197 functionele eisen opgesteld.

Voor de volledige lijst met functionele eisen zie bijlage A en *Functionele Requirements v1.0.xlsx*.

Prioriteiten:

Categorie	Aantal	Toelichting
must have	79	Minimale functionaliteit voor een werkbaar product (MVP)
should have	62	Hoge prioriteit, maar niet vereist voor een bruikbaar product
could have	40	Optie die alleen wordt meegenomen als er tijd over is
won't have	16	Geen prioriteit of niet wenselijk
TOTAAL	**197**	



Categorieën:

Categorie	Aantal	Toelichting
Authenticatie	11	Toegang tot het systeem
Beheer	7	Functionaliteit t.b.v. Beheer
Chat	25	Chat functie
Coördinatie	30	Functionaliteit voor coördinatie van een zoekactie
Informatie	12	Algemene informatie
Instellingen	2	Persoonlijke instellingen
Kaart	40	Functionaliteit tot kaarten
Kwaliteitseis	3	Kwaliteitseisen
Politie	13	Eventuele functionaliteit voor de politieondersteuning
Support	14	Ondersteunende taken
Taken	6	Functionaliteit om taken te verdelen
Usability	2	Bruikbaarheidseisen
Vondsten	7	Melden van vondsten
Voorwaarden	2	Acceptatie van voorwaarden door gebruikers
Zoeken	23	Functionaliteit t.b.v. het zoeken
TOTAAL	**197**	

Customer journey fase:

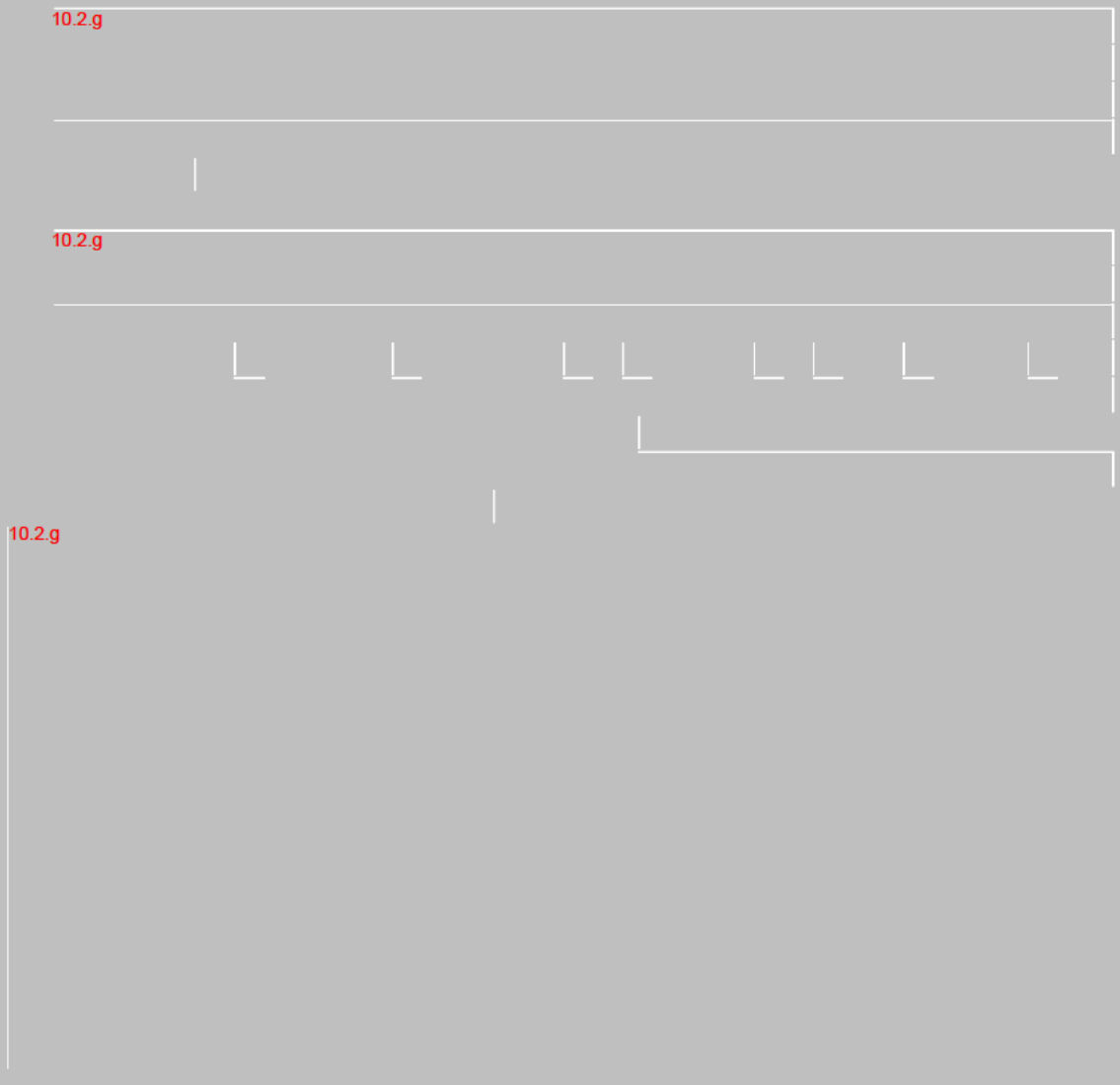
Categorie	Aantal	Toelichting
[Hele proces]	33	Algemeen, niet gebonden aan een customer journey stap
Beheer	10	Beheer activiteiten
Lopende zoekactie	95	Gedurende een lopende zoekactie
Onboarding	14	Onboarding van zoekers
Overdracht	14	Overdracht van data aan ondersteunende partijen zoals Politie
Registratie	8	Registratie van gebruikers
Start zoekactie	11	Starten van een zoekactie
Start zoeken	7	Starten met zoeken
Stop zoekactie	3	Stoppen van een zoekactie
Stop zoeken	2	Stopen met zoeken
TOTAAL	**197**	

Todo

5 EIGENAARSCHAP

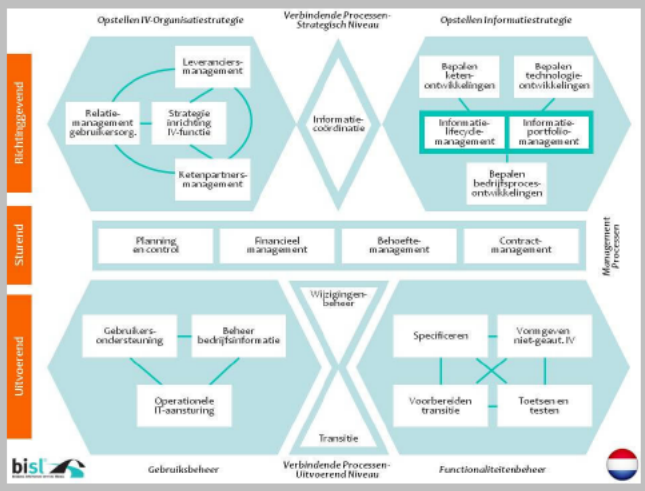
5.1 JURIDISCHE ENTITEIT

Bij de exploitatie zullen verschillende partijen betrokken zijn. Het is van primair belang dat de verantwoordelijkheden bij deze partijen goed ingevuld worden. Er zal een partij eigenaar moeten zijn en de onderaannemers moeten kunnen aansturen om gezamenlijk een succesvol en betrouwbaar platform kunnen maken.



5.2 BEHEERPROCESSSEN

Wanneer het platform live gaat en beschikbaar wordt voor het brede publiek, zullen er ook diverse beheeractiviteiten ingericht dienen te worden. 10.2.e. raadt aan om de beheerafspraken in te richten volgens het BiSL model. Business Information Services Library (BiSL), voorheen Business Information Service Management Library, is een raamwerk voor het uitvoeren van functioneel beheer en informatiemanagement.



5.3 FINANCIERING

Uitgangspunten:

- Geen winstoogmerk
- Onafhankelijk
- Geen inkomsten uit data verkoop, gebruikerslicenties en reclame
- Minimale inkomsten uit platform (initieel)
    - Directe kosten zijn hoger dan directe inkomsten
    - Externe financiering noodzakelijk

Mogelijkheden:

- Subsidies & donaties
- Licenties

Relevante kenmerken:

- Zekerheid van (structurele) inkomsten
- Initiële (ontwikkel)kosten en exploitatiekosten
- Aanbestedingswet 2012 (AW 2012)
- Maatschappelijk draagvlak
- Is financiering door overheid en eigenaarschap bij andere (commerciële) organisaties belastingtechnisch overdraagbaar?

6 KWALITEITSEISEN

Naast de functionele eisen, is het ook noodzakelijk om de kwaliteitseisen in kaart te brengen. Hiermee kan de kwaliteit, van het opgeleverde product objectief getoetst worden.
Een belangrijk onderdeel hierbij, zijn ook de beveiligingseisen. Deze worden daarom onder een separaat hoofdstuk behandeld.

De beveiligingseisen zijn opgesteld aan de hand van de ISO 25010 standaard:

De kwaliteitseisen steen beschreven in Bijlage B en het document *Niet-Functionele Requirements (v1.0).xlsx*

Categorie	Aantal
Betrouwbaarheid	15
Beveiligbaarheid	6
Bruikbaarheid	12
Functionele geschiktheid	2
Onderhoudbaarheid	11
Overdraagbaarheid	13
Prestatie-efficiëntie	5
Voldoening	3
TOTAAL	**67**

6.1 BEVEILIGINGSRICHTLIJNEN

Security aspecten zijn opgesteld door [redacted]. De beveiligingsrichtlijnen richten zich op ICT-aspecten, maar ook de ondersteunde processen. Er zijn zo'n 300 relevante richtlijnen beschreven met betrekking tot ontwikkeling en beheer.

Zie hiervoor het document *ICT-beveiligingsrichtlijnen voor Sarea webapplicaties en mobiele app.xlsx*.

Hiervoor zijn de volgende bronnen gebruikt:

- Bestaande documentatie
- Functionele eisen
- Niet-functionele eisen
- Risk Assessment
- OWASP Top 10
- NCSC ICT-beveiligingsrichtlijnen voor mobiele apps
- NCSC ICT-beveiligingsrichtlijnen voor webapplicaties
- Input projectteam
- Review/ aanvullende vragen projectteam

7 PRIVACY ASPECTEN

7.1 INLEIDING

7.1.1 AANPAK

Privacyaspecten zijn getoetst door 10.2.e. 10 2.g

DPIA uitgevoerd op basis van:

- Bestaande documentatie
- Onderzoeksrapporten 10.2.g
- Functionele requirements
- Risk Assessment
- Input projectteam
- Review/ aanvullende vragen projectteam

7.1.2 DISCLAIMER VOORAF

De Algemene verordening gegevensbescherming (AVG) is geschreven als een open norm. Dat wil zeggen dat verwerkingsverantwoordelijken zelf verantwoordelijk zijn voor het maken van beoordelingen, afwegingen en keuzes ten aanzien van de verwerking van persoonsgegevens. De AVG verbiedt niet zo veel, maar stelt voorwaarden waaraan de verwerking van persoonsgegevens moet voldoen.

Als gevolg hiervan kan er onzekerheid ontstaan over de rechtmatigheid van een verwerking. Een verwerkingsverantwoordelijke kan een keuze maken op grond van een eigen afweging, die achteraf door een rechter of toezichthoudende autoriteit wordt betwist. Naarmate de AVG langer in werking is, worden afwegingskaders duidelijker doordat toezichthouders richtlijnen uitbrengen of jurisprudentie ontstaat door uitspraken in juridische procedures.

Op voorhand kan niet worden uitgesloten dat een risicovolle verwerking zoals in de Sarea-applicatie beoogd ter discussie zal worden gesteld. Hoe beter de applicatie op voorhand is beschreven, hoe kleiner de kans dat achteraf problemen ontstaan.

7.1.3 OVERWEGINGEN VOORAF

Verwerkingsverantwoordelijkheid

De studenten van de 10.2.g staan in hun onderzoeksrapporten terecht uitvoerig stil bij de verwerkingsverantwoordelijkheid. Conclusie van één van de rapporten is dat er sprake kan zijn van een gezamenlijke verwerkingsverantwoordelijkheid van de aanbieder van de applicatie en de coördinator.

De verwerkingsverantwoordelijke is degene die doel en middelen van de verwerking bepaalt en verantwoordelijkheid draagt voor het aantoonbaar naleven van de AVG. De verantwoordelijke is aanspreekbaar en aansprakelijk voor de gevolgen van de verwerking. Betrokkenen en toezichthouders zullen de verantwoordelijke aanspreken bij vragen of klachten over de verwerking.

Bij grove schendingen kan de Autoriteit Persoonsgegevens de verantwoordelijke een boete of andere sanctie opleggen.
Zo bezien moet je vermijden dat een bezorgde vriend of familielid, die een zoekactie opstart, zich onbewust de verwerkingsverantwoordelijkheid op de hals haalt. Je kunt niet van hem verwachten dat hij de consequenties daarvan overziet.
Het advies is om de verantwoordelijkheid dan ook volledig bij de aanbieder van de applicatie te leggen. Dat betekent overigens wel dat de verwerkingsverantwoordelijke veiligheidsmechanismen moet inbouwen om te voorkomen dat er te veel persoonsgegevens of te gevoelige gegevens bekend worden gemaakt.

Algoritme ter bepaling van het zoekgebied

Een complicerende factor is de inzet van een algoritme. Eén van de rapporten wijdt uitvoerig uit over het gebruik van een algoritme om de zoekinspanning te optimaliseren. Het gebruik van dit soort technologie wordt zowel in de AVG als door de verschillende toezichthouders aangemerkt als hoog risico voor de rechten en vrijheden van betrokkenen. Algoritmes hebben nogal eens bedoelde of onbedoelde bijeffecten en op enig moment zijn ze zo complex dat vrijwel niemand nog echt begrijpt wat ze doen. De voorbeelden hiervan kennen we uit de media.

De meerwaarde of noodzaak van het gebruik van een dergelijk algoritme zal zorgvuldig moeten worden uitgewerkt.

7.2 SAMENVATTING VAN AANBEVELINGEN

In de volgende hoofdstukken zijn aanbevelingen opgenomen om de privacy van betrokkenen te waarborgen. Omwille van het overzicht zijn de aanbevelingen hierna samengevat:

1. Maak duidelijk welk businessmodel het platform kent. Wie betaalt uiteindelijk de rekening? Zijn er andere financieringsstromen of opbrengsten, bijvoorbeeld uit advertenties? Zo niet, beschrijf dat dan ook.
2. Zorg ervoor dat de gegevens de Europese Economische Ruimte niet verlaten. Vooralsnog moet het Verenigd Koninkrijk gerekend worden buiten de EER.
3. Beschrijf de beoogde inzet van het algoritme in de tooling, waarom dit noodzakelijk is en hoe de privacy van betrokkenen wordt beschermd tegen ongewenste of onvoorziene bijeffecten van het algoritme.
4. Richt het platform zo in dat persoonsgegevens kunnen worden verwijderd na het staken van een zoekactie of na het intrekken van toestemming door de betrokkene. Wanneer gegevens verder worden verwerkt voor analytische of statistische doeleinden (bijv. in het algoritme), anonimiseer de gegevens dan. Anonieme gegevens kunnen (uit oogpunt van de AVG) onbeperkt verder verwerkt worden.
5. Informeer coördinatoren en zoekers op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke manier over alle beoogde verwerkingen van persoonsgegevens (artikel 12 AVG).
6. Beschrijf hoe zoekgegevens, bijvoorbeeld het GPS-track van een zoeker, kan worden bewaard zonder persoonsgegevens, dus geanonimiseerd, nadat de zoeker zijn toestemming heeft ingetrokken. Dit suggereert een harde ontkoppeling van persoonsgegevens en zoekgegevens.
7. Voorkom dat bijzondere persoonsgegevens van de vermiste bekend worden gemaakt. Bouw een controlestap in voordat persoonsgegevens van de vermiste bekend worden gemaakt. Beperk de bekend te maken gegevens tot de gegevens die daadwerkelijk relevant zijn voor het opzetten van een zoekactie.
8. Tref maatregelen zodat persoonsgegevens alleen worden verzameld in de context van de zoekactie. Pas hierbij de principes “privacy by default” en “privacy by design” toe.
9. Beschrijf welke minder impactvolle acties moeten zijn uitgevoerd alvorens een zoekactie kan worden opgestart.
10. Richt voorzieningen in voor coördinator en zoekers om hun rechten uit te oefenen

11. Bereid je zorgvuldig voor op het scenario dat de gezochte persoon zich meldt met het verzoek de zoekactie te staken. Wees voorbereid op reacties van coördinator, zoekers, de samenleving. Wapen je tegen een publiciteitsstorm in de (sociale) media.

7.3 A: BESCHRIJVING KENMERKEN GEGEVENSVERWERKINGEN

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Het doel is de ontwikkeling van een platform, bestaande uit een website en een app, die het mogelijk maakt een gecoördineerde zoekactie op touw te zetten naar een vermiste persoon. De ontwikkeling is een reactie op de ongecoördineerde burgerinitiatieven waarbij bezorgde burgers zelfstandig of met een groep op zoek gaan naar een vermiste persoon. Omdat coördinatie ontbreekt zijn dit soort zoekacties, hoewel gestart vanuit oprechte betrokkenheid, vaak weinig effectief of soms zelfs schadelijk omdat sporen of bewijsmateriaal wordt beschadigd.

Tegelijkertijd kan een gecoördineerde zoekactie een enorme capaciteit op de been brengen om in korte tijd een groot gebied te doorzoeken. Het doel van het initiatief is om een platform te bouwen om dit soort burgerzoekacties te faciliteren, waardoor de zoekactie gestructureerd kan worden aangepakt en gestuurd op basis van ervaringen uit eerdere zoekacties.

Deze notitie behandelt de privacy-aspecten van het platform. In een zoekactie is sprake van diverse categorieën van betrokkenen: de gezochte persoon, een coördinator/initiatiefnemer, een groep zoekers, beheerders van het platform. Van deze betrokkenen worden persoonsgegevens verwerkt. Denk aan de persoonskenmerken van de vermiste persoon, de GPS-tracking van een zoeker, loggegevens van systeemmutaties. Al deze persoonsgegevens moeten verwerkt worden binnen de wettelijke kaders van de AVG. Wanneer er sprake is van een mogelijk misdrijf, treedt de Wet politiegegevens in werking. Deze notitie verkent de privacy-aspecten van het beoogde platform en geeft aanbevelingen en randvoorwaarden mee aan de ontwikkelaars van het platform.

2. Persoonsgegevens

Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificatienummer.

Op grond van de functionele specificaties (versie 0.8) kunnen de volgende rollen, vergelijkbaar met categorieën van betrokkenen, worden geïdentificeerd:

Rol	Toelichting
Bezoeker	Een onbekende gebruiker (dus zonder account)
Zoeker	Een persoon die mee kan gaan zoeken
Coördinator	De coördinator van een zoekactie (mogelijk meerdere per zoekactie)
Politie ondersteuner	Medewerker(s) van de Politie, welke mee kan kijken in de zoekactie
Servicedesk 1e lijns	Beantwoorden van algemene vragen
Servicedesk 2e lijns	Blokkeren van accounts, verwijderen van accounts
Security Officer	Afhandelen van beveiligingsincidenten, bewaken van beveiligingsrisico's
Platform beheerder	Instellen en configureren van het platform, bewaken
Content beheerder	Onderhoud teksten + e-mails

In bovenstaand overzicht mist de betrokkene voor wie de grootste impact op de privacy mag worden verwacht, namelijk de **vermiste persoon**.

Van elk van deze categorieën van betrokkenen worden in meer of mindere mate persoonsgegevens verwerkt. Van wezenlijke risico's voor de privacy is echter alleen sprake bij de coördinator, de zoeker en de vermiste persoon. Voor de overige betrokkenen volstaan naar mijn oordeel privacy- en beveiligingsmaatregelen zoals die vandaag de dag redelijkerwijs mogen worden verwacht voor websitebezoekers of in de beroepsmatige context. Deze notitie zal zich verder dan ook beperken tot de categorieën van betrokkenen met wezenlijke risico's voor de privacy.

In de tabel hieronder wordt bovenstaande tabel aangevuld met de categorieën van persoonsgegevens die worden verwerkt.

Rol	Toelichting	Persoonsgegevens
Bezoeker	Een onbekende gebruiker (dus zonder account)	
Zoeker	Een persoon die mee kan gaan zoeken	Naam, e-mailadres, mobiel telefoonnummer, …
Coördinator	De coördinator van een zoekactie (mogelijk meerdere per zoekactie)	Naam, e-mailadres, mobiel telefoonnummer, …
Vermiste persoon	De persoon waarnaar gaat worden gezocht	Naam, persoonskenmerken, foto, kleding, bezittingen, laatst bekende verblijfplaats, …
Politie ondersteuner	Medewerker(s) van de Politie, welke mee kan kijken in de zoekactie	
Servicedesk 1e lijns	Beantwoorden van algemene vragen	
Servicedesk 2e lijns	Blokkeren van accounts, verwijderen van accounts	
Security Officer	Afhandelen van beveiligingsincidenten, bewaken van beveiligingsrisico's	
Platform beheerder	Instellen en configureren van het platform, bewaken	
Content beheerder	Onderhoud teksten + e-mails	
Bezoeker	Een onbekende gebruiker (dus zonder account)	
Zoeker	Een persoon die mee kan gaan zoeken	Naam, e-mailadres, mobiel telefoonnummer, …
Coördinator	De coördinator van een zoekactie (mogelijk meerdere per zoekactie)	Naam, e-mailadres, mobiel telefoonnummer, …
Vermiste persoon	De persoon waarnaar gaat worden gezocht	Naam, persoonskenmerken, foto, kleding, bezittingen, laatst bekende verblijfplaats, …

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

De volgende gegevensverwerking kunnen op basis van de functionele specificaties worden onderkend:

- Het registeren van een gebruiker en beschikbaar houden van de gegevens
- Het opstarten van een zoekactie, het vastleggen van kenmerken van de vermiste persoon
- Het uitvoeren en coördineren van een zoekactie, volgen en vastleggen van GPS-locatie van zoekers

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

Verwerkingsdoel is het faciliteren van een gecoördineerde zoekactie naar een vermiste persoon.

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Facilitator van het platform is vooralsnog het bedrijf 10.2.g B.V. De facilitator is **verwerkingsverantwoordelijke** voor alle verwerkingen van persoonsgegevens op het platform (zie de opmerking op pagina 1 over de rol van verwerkingsverantwoordelijke).

Het platform wordt waarschijnlijk gehost op een cloud-omgeving van een externe leverancier. Deze leverancier kan waarschijnlijk worden gekwalificeerd als **verwerker**. Sluit in dat geval een verwerkersovereenkomst met deze partij.
Op enig moment kan de politie een rol krijgen in de zoekactie, bijvoorbeeld wanneer er mogelijk sprake is van een misdrijf. De politie is in dit geval een **ontvanger**. De politie zal de persoonsgegevens verder verwerking op grond van de eigen bevoegdheid.

6. Belangen bij de gegevensverwerkingen
Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.
Het belang van de verwerkingsverantwoordelijke is het mogelijk maken van een gecoördineerde zoekactie naar een vermiste persoon.

AANBEVELING: Maak duidelijk welk businessmodel het platform kent. Wie betaalt uiteindelijk de rekening? Zijn er andere financieringsstromen of opbrengsten, bijvoorbeeld uit advertenties? Zo niet, beschrijf dat dan ook.

7. Verwerkingslocaties
Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.
De zoekacties vinden plaats in Nederland. Alle gegevensverwerkingen met betrekking tot zoekers, vermiste personen, coördinatoren etc. vinden plaats in Nederland. De gegevens in de app en op de website zijn opgeslagen in een cloud-omgeving.

AANBEVELING: Zorg ervoor dat de gegevens de Europese Economische Ruimte niet verlaten. Vooralsnog moet het Verenigd Koninkrijk gerekend worden buiten de EER.

8. Technieken en methoden van de gegevensverwerkingen
Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi¬) geautomatiseerde besluitvorming, profilering of big data¬verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.
De zoekinspanning wordt geoptimaliseerd door middel van een algoritme dat zoekers kan aansturen in de richting van locaties met een hogere vindkans. Het gebruik van dit soort technologie wordt zowel in de AVG als door de verschillende toezichthouders aangemerkt als hoog risico voor de rechten en vrijheden van betrokkenen. Algoritmes hebben soms bedoelde of onbedoelde bijeffecten en kunnen op enig moment zo complex zijn dat vrijwel niemand nog echt doorziet wat ze doen. De voorbeelden hiervan kennen we uit de media.
Het is zaak om in de uitwerking glashelder te maken wat de werking van een beoogd algoritme is, waarom de inzet van zo'n algoritme noodzakelijk of tenminste van grote meerwaarde is voor het beoogde doel en hoe de privacy van alle betrokkenen geborgd is, wanneer bijvoorbeeld zoekgegevens aan het algoritme worden gevoerd ter lering. Denk na over de ontkoppeling van persoonsgegevens van technische gegevens, zodat bijvoorbeeld op enig moment niet meer te achterhalen wie welk zoekpad heeft gelopen. Enquêtetools doen dat bijvoorbeeld door twee separate databases in te richten, één met contactgegevens van de geïnterviewden en één met de antwoorden, waarbij er geen link bestaat tussen die twee. Dan nog is er natuurlijk een risico van singling-out.

AANBEVELING: beschrijf de beoogde inzet van het algoritme in de tooling, waarom dit noodzakelijk is en hoe de privacy van betrokkenen wordt beschermd tegen ongewenste of onvoorziene bijeffecten van het algoritme.

9. Juridisch en beleidsmatig kader

Benoem de wet¬ en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

Toepasselijkheid van de AVG

De AVG is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit (artikel 2, lid 2, onderdeel c), waarbij in overweging 18 nog wat verder gespecificeerd is dat dit een "louter persoonlijke of huishoudelijke activiteit die als zodanig geen enkel verband houdt met een beroeps – of handelsactiviteit." Tevens stelt deze overweging dat de verordening wel van toepassing is op verwerkingsverantwoordelijken die middelen verschaffen voor dergelijke activiteiten.

Een zoekactie, geïnitieerd door een particulier persoon, kan daardoor onder voorwaarden buiten de werking van de AVG worden uitgevoerd. Zodra je echter een middel gaat aanbieden om die zoekactie te faciliteren is de AVG wel degelijk van toepassing.

Naast de AVG en eventueel de Wet politiegegevens is de Grondwet worden genoemd, die iedereen het recht geeft op de eerbiediging van de persoonlijke levenssfeer (artikel 10). Iedereen moet beschermd worden tegen ongewenste en onrechtmatige inmenging door overheden of organisaties. Deze inmenging kan alleen met een wettelijke basis.

Daarnaast heeft iedereen recht op vrijheid (artikel 15). Deze vrijheid gaat zover dat iemand uit vrije wil mag verdwijnen.

Het feit dat bovengenoemde rechten zijn aangemerkt als grondrecht, betekent dat deze zwaar moeten wegen bij de beoordeling of een inbreuk op de persoonlijke levenssfeer gerechtvaardigd is.

Het Burgerlijk Wetboek, boek 1, titel 18, voorziet in gevallen van vermissing, maar gaat vooral over de afwikkeling van de belangen na langere tijd. Hieraan kan geen bruikbare informatie worden ontleend voor deze beoogde verwerking.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk voor het doel van de verwerking. Soms bestaat er een verplichting tot bewaren, bijvoorbeeld vanuit de Archiefwet of om fiscale redenen. Dat is hier niet aan de orde.

Dit impliceert dat de persoonsgegevens, verzamelt in het kader van een specifieke zoekactie, verwijderd moeten worden nadat de zoekactie is afgesloten. Bijvoorbeeld omdat de vermiste weer is opgedoken of is gevonden.

Persoonsgegevens van zoekers of coördinatoren mogen langer worden bewaard, mits de betrokkene daar zelf toestemming voor heeft gegeven, bijvoorbeeld om opnieuw deel te nemen aan een volgende zoekactie. Wanneer die toestemming wordt ingetrokken, moeten persoonsgegevens van coördinatoren en zoekers worden verwijderd.

AANBEVELING: Richt het platform zo in dat persoonsgegevens kunnen worden verwijderd na het staken van een zoekactie of na het intrekken van toestemming door de betrokkene. Wanneer gegevens verder worden verwerkt voor analytische of statistische doeleinden (bijv. in het algoritme), anonimiseer de gegevens dan. Anonieme gegevens kunnen (uit oogpunt van de AVG) onbeperkt verder verwerkt worden.

7.4 B. BEOORDELING RECHTMATIGHEID GEGEVENSVERWERKINGEN

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Iedere verwerking van persoonsgegevens moet gebaseerd zijn op één van de zes grondslagen uit de AVG.

Zoekers en coördinatoren

Voor de verwerking van persoonsgegevens van zoekers en coördinatoren is de grondslag toestemming toepasbaar. Om rechtsgeldig toestemming te verkrijgen stelt de AVG-voorwaarden aan de omstandigheden wordt verkregen. Toestemming moet door middel van een **actieve handeling**, en **vrijelijk**, **specifiek**, **geïnformeerd** en **ondubbelzinnig** worden gegeven. Voor het verwerken van persoonsgegevens van minderjarigen (< 16 jaar) moeten de ouders toestemming geven. Bovenstaande vetgedrukte begrippen worden hierna toegelicht.

- Actieve handeling: Toestemming vereist een bewuste handeling van de betrokkene. Daaronder valt niet een vooraf aangevinkt veld of een toestemming die impliciet is opgenomen in gebruikersvoorwaarden. De betrokkene moet door een daadwerkelijke handeling, bijvoorbeeld het aanvinken van een veld, zijn toestemming verlenen
- Vrijelijk: De betrokkene moet daadwerkelijk vrij zijn om toestemming te verlenen. Het niet geven van toestemming mag geen directe of indirecte nadelige gevolgen hebben voor de betrokkene of de betrokkene belemmeren in zijn rechten. Er mag geen sprake zijn van een gezagsverhouding tussen betrokkene en verwerkingsverantwoordelijke.
- Specifiek: toestemming moet gegeven kunnen worden voor de specifieke verwerking. Voor iedere verdere verwerking, die geen logisch en onlosmakelijk gevolg is van de oorspronkelijke verwerking, dient opnieuw toestemming te worden gevraagd.
- Geïnformeerd: de betrokkene dient zich bewust te zijn waarvoor hij toestemming verleent. Hier heeft de verantwoordelijke de taak om de betrokkene goed te informeren over de beoogde verwerking van persoonsgegevens en de manier waarop de betrokkene invloed kan uitoefenen, bijvoorbeeld door toestemming in te trekken of de verwerking tijdelijk te stoppen.
- Ondubbelzinnig: toestemming mag niet zijn “weggemoffeld” in gebruikersvoorwaarden of verkregen zijn op basis van dubieuze voorwaarden.

Toestemming is te allen tijde intrekbaar. Na het intrekken van toestemming door de betrokkene dient iedere verwerking van persoonsgegevens te worden gestaakt en is er geen grond meer voor bewaring van de persoonsgegevens. Deze dienen na intrekking van de toestemming zo snel mogelijk vernietigd te worden.

Coördinatoren en zoekers nemen geheel vrijwillig en uit intrinsieke motivatie deel aan een zoekactie. De kans dat iemand hiertoe gedwongen wordt, is verwaarloosbaar. Toestemming is daarom, rekening houdend met bovengenoemde voorwaarden, een passende grondslag voor de verwerking van persoonsgegevens van coördinatoren en zoekers.

AANBEVELING: Informeer coördinatoren en zoekers op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke manier over alle beoogde verwerkingen van persoonsgegevens (artikel 12 AVG).

AANBEVELING: Beschrijf hoe zoekgegevens, bijvoorbeeld het GPS-track van een zoeker, kan worden bewaard zonder persoonsgegevens, dus geanonimiseerd, nadat de zoeker zijn toestemming heeft ingetrokken. Dit suggereert een harde ontkoppeling van persoonsgegevens en zoekgegevens.

Vermiste persoon

De rechtsgrond voor de verwerking van de persoonsgegevens van de vermiste persoon is het meest complex. Afhankelijk van de situatie is een andere grondslag toepasbaar, maar de situatie is op voorhand niet altijd duidelijk. Aan de hand van de mogelijke situaties zijn de volgende grondslagen toepasbaar.

Meerderjarige vermiste, slachtoffer van ongeval of misdrijf

In de situatie dat een vermiste slachtoffer is geworden van een ongeval of misdrijf, mag worden aangenomen dat de betrokkene niet voor zijn eigen belangen kan opkomen. In dit geval voorziet de AVG in de grondslag "Vitaal belang". Op voorhand is echter niet met zekerheid vast te stellen dat de betrokkene daadwerkelijk slachtoffer is. In de functionaliteit zou aan de hand van een aantal controlevragen moeten worden vastgesteld hoe waarschijnlijk het is dat de vermiste persoon niet uit vrije wil is vertrokken. Wanneer het waarschijnlijk is dat de vermiste persoon niet uit vrije wil is vertrokken, kan worden verwerkt op grond van de grondslag vitaal belang.

Meerderjarige vermiste, vertrokken uit vrije wil

Hoe pijnlijk en wrang voor de achterblijvers het ook is, iedereen heeft het recht om te verdwijnen. Wanneer iemand uit vrij wil vertrekt met onbekende bestemming, is de betrokkene prima in staat om op te komen voor zijn eigen belangen. De grondslag vitaal belang is dus niet toepasbaar. Betrokkene zal in dit geval ook geen toestemming geven. Resteert alleen nog de grondslag "gerechtvaardigd belang". Hiervoor moet worden aangetoond dat de verwerkingsverantwoordelijke een belang heeft dat groot genoeg is om de inbreuk te rechtvaardigen. Dat houdt waarschijnlijk geen stand. Geconcludeerd moet worden dat er in deze situatie geen passende grondslag voor de verwerking van persoonsgegevens van de betrokkene voorhanden is. De verwerking is dan onrechtmatig.

Hierin schuilt een groot risico voor de betrokkene en daarmee voor beoogde toepassing. Omdat de situatie van de vermiste persoon niet op voorhand kan worden bepaald, kan niet worden uitgesloten dat de verwerking onrechtmatig is. Een toezichthoudende autoriteit zal dit zeer kritisch benaderen en mogelijk zelfs verbieden. Om de kans op een verwerkingsverbod zo veel mogelijk te beperken, moeten maatregelen getroffen worden om de te verwerken persoonsgegevens van de vermiste zo beperkt mogelijk te houden.

Minderjarige vermiste

In geval van een minderjarige vermiste (< 16 jaar) kunnen de ouders toestemming geven voor de verwerking, ongeacht de reden van de vermissing. Hier gelden de hiervoor genoemde voorwaarden.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden en dient te worden vermeden. Ook hierin schuilt een aanzienlijk risico. Voorstelbaar is dat een bezorgd familielid een uitvoerige beschrijving van de vermiste gaat geven, met vermelding van allerlei persoonlijke details. Voor het opstarten van een zoekactie volstaan echter algemene uiterlijke kenmerken, een foto, kenmerkende bezittingen en laatst bekende verblijfplaats van de vermiste. De zoekers hoeven geen sluitende identificatie uit te kunnen voeren.

AANBEVELING: voorkom dat bijzondere persoonsgegevens van de vermiste bekend worden gemaakt. Bouw een controlestap in voordat persoonsgegevens van de vermiste bekend worden gemaakt. Beperk de bekend te maken gegevens tot de gegevens die daadwerkelijk relevant zijn voor het opzetten van een zoekactie.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De verwerkingsverantwoordelijke dient de verwerking van persoonsgegevens te beperken tot zover noodzakelijk voor het beoogde doel, te weten een specifieke zoekactie. Het doel is beschreven bij onderdeel 4 van deze notitie.

Coördinator en zoekers

In de functionele specificaties wordt gesproken over een algoritme dat de zoekacties kan ondersteunen. Verdedigbaar is dat dit verenigbaar is met het oorspronkelijke doel, omdat hiermee toekomstige zoekacties kunnen worden verbeterd. Wanneer een harde ontkoppeling kan plaatsvinden tussen persoonsgegevens en zoekgegevens, en zoekgegevens volledig geanonimiseerd zijn, vervalt dit argument en kan verdere verwerking plaatsvinden.

Vermiste persoon

Wanneer een zoekactie wordt gestaakt, vervalt het doel voor de verwerking van de persoonsgegevens van de vermiste persoon.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

a. *Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?*
b. *Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.*

Coördinator en zoekers

Hoewel coördinator en zoekers vrijwillig deelnemen aan een zoekactie, geldt ook hier dat de gegevensverwerking proportioneel en subsidiair moet zijn. Dit geldt voor de registratie van coördinatoren en zoekers (welke gegevens heb je hiervoor echt nodig?) maar ook voor het verzamelen van gegevens tijdens de zoekactie. Het is wenselijk het zoekpad van de zoeker vast te leggen, zodat bepaald kan worden waar al gezocht is. Het volgen van de zoeker buiten de context van een zoekactie is echter uit den boze.

Dit kan bereikt worden door bijvoorbeeld de gegevensverwerking te beperken tot de tijdvensters waarbinnen een zoekactie wordt gehouden, door zoekers niet in de eigen woonomgeving te traceren, door de app alleen werkzaam te laten zijn wanneer deze door de gebruiker “aan” is gezet.

Vermiste persoon

Om te bepalen of een verwerking proportioneel is, moet worden aangetoond dat de beoogde inbreuk in evenredige verhouding staat tot het verwerkingsdoel. Ook hier valt die beoordeling anders uit al naar gelang de situatie van de vermiste. Het opsporen van een verondersteld slachtoffer

van een ongeval of misdrijf, rechtvaardigt een verdergaande verwerking van persoonsgegevens. Omdat dit echter niet op voorhand te bepalen is, dient de verwerking in beginsel een zo minimaal mogelijke inbreuk op de privacy van de vermiste te veroorzaken. Proportioneel lijkt hier dan vooralsnog alleen de verwerking van uiterlijke kenmerken, kleding en accessoires, laatst bekende verblijfplaats.

Subsidiariteit gaat over het bereiken van het doel met minder vergaande middelen. Hierbij kan in bij deze verwerking gedacht worden aan:

- Is gepoogd contact te leggen met de vermiste?
- Zijn mogelijke waarschijnlijke verblijfplaatsen doorzocht?
- Is contact gelegd met familie, vrienden, bekenden, anderen in de sociale omgeving van betrokkene?
- Is navraag gedaan bij zorgverleners en/of ziekenhuizen in de omgeving?

AANBEVELING: tref maatregelen zodat persoonsgegevens alleen worden verzameld in de context van de zoekactie. Pas hierbij de principes “privacy by default” en “privacy by design” toe.

AANBEVELING: Beschrijf welke minder impactvolle acties moeten zijn uitgevoerd alvorens een zoekactie kan worden opgestart.

15. Rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.
Betrokkenen hebben recht op inzage, gegevenswissing, rectificatie, verwerkingsbeperking en bezwaar. In de applicatie moeten voorzieningen worden getroffen om de uitoefening van deze rechten mogelijk te maken.

Coördinator en zoekers

Voor coördinator en zoekers zal de applicatie voorzieningen moeten bevatten om hun rechten uit te oefenen.

Vermiste persoon

Ook hier tekent zich een bijzondere situatie af in relatie tot de vermiste persoon. Wanneer de vermiste het slachtoffer is geworden van een ongeval of misdrijf, zal hij zijn rechten niet kunnen uitoefenen.
Ouders kunnen de rechten uitoefenen namens hun minderjarige kind.
In de situatie dat een meerderjarige vermiste uit vrije wil is verdwenen, zal deze wellicht zijn rechten willen uitoefenen om de zoekactie te laten staken. Dit levert wel een buitengewoon complexe situatie op. Er doemen een aantal heel lastige vragen op:

- Hoe kan de vermiste zich melden om zijn rechten uit te oefenen?
- Hoe wordt de identiteit van degene die zegt de vermiste te zijn geverifieerd? Voorstelbaar is dat een dader van een misdrijf zich uitgeeft voor de vermiste om een zoekactie te laten staken.
- Hoe ben je voorbereid op de lastige boodschap aan coördinator en zoekers dat de vermiste vrijwillig is vertrokken en niet gevonden wil worden? En dat de zoekactie dus moet worden gestaakt.
- Ben je bestand tegen de druk uit deze groep en de samenleving om toch verder te zoeken?

AANBEVELING: Richt voorzieningen in voor coördinator en zoekers om hun rechten uit te oefenen

AANBEVELING: Bereid je zorgvuldig voor op het scenario dat de gezochte persoon zich meldt met het verzoek de zoekactie te staken. Wees voorbereid op reacties van coördinator, zoekers, de samenleving. Wapen je tegen een publiciteitsstorm in de (sociale) media.

7.5 C. BESCHRIJVING EN BEOORDELING RISICO'S VOOR DE BETROKKENEN

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

a. Welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en
b. Vrijheden van de betrokkenen;
c. De oorsprong van deze gevolgen;
d. De waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
e. De ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

De risico's van de voorgenomen verwerking zijn in de voorgaande paragrafen van dit document beschreven en voorzien van aanbevelingen om de risico's te behandelen. Advies is om deze aanbevelingen op te volgen en in de vorm van maatregelen te implementeren in de applicatie. Daarna kan een risicoanalyse worden uitgevoerd om te bepalen hoe omvangrijk de restrisico's zijn en welke aanvullende maatregelen noodzakelijk zijn.

Ongeacht de te implementeren maatregelen zijn twee risico's geïdentificeerd die hoe dan ook een rol spelen:

- Een **groot risico** voor de betrokkene en daarmee voor beoogde toepassing: Omdat de situatie van de vermiste persoon niet op voorhand kan worden bepaald, kan niet worden uitgesloten dat de verwerking onrechtmatig is. Een toezichthoudende autoriteit zal dit zeer kritisch benaderen en mogelijk zelfs verbieden.
- Het verwerken van bijzondere persoonsgegevens is in beginsel verboden en dient te worden vermeden. Hierin schuilt een **aanzienlijk risico**. Voorstelbaar is dat een bezorgd familielid een uitvoerige beschrijving van de vermiste gaat geven, met vermelding van allerlei persoonlijke details.

7.6 D. BESCHRIJVING VOORGENOMEN MAATREGELEN

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevens-verwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel.
Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Zie toelichting bij onderdeel 16.

7.7 VERDIEPINGSVRAGEN

Wat kunnen zoekers met elkaar delen en van elkaar zien? Uiteraard mogelijk weer met expliciete goedkeuring van de zoeker.

1. Directe berichten sturen (zonder expliciete controle/goedkeuring van de coördinator). Ze moeten hiervoor dus ook in de lijst met namen van zoekers kunnen inzien.
2. Foto's van de zoeker, bijvoorbeeld op de kaart of bij een bericht. Dit is wenselijk omdat de zoekers elkaar dan kunnen herkennen.
3. Actuele locatie van zoekers. Hiermee kun je zoekers in de buurt vinden. Kan natuurlijk vrij gevoelig zijn, maar Snap, Facebook en andere apps bieden deze mogelijkheid ook.

Eigenlijk moet je de vraag omdraaien. Wat is functioneel en noodzakelijk om het doel van de applicatie te kunnen bereiken? Daarmee kom je wellicht op een set basisfuncties die noodzakelijk zijn om een zoekactie in gang te zetten en een set extra, additionele functies die het gemakkelijker maken.

Het voordeel van werken met toestemming is dat je eventueel per gewenste functie toestemming kunt uitvragen. In basis mag je verwachten dat de app van jou als zoeker je naam en contactgegevens verwerkt, je zoekpad vastlegt (wanneer ingeschakeld en alleen voor de duur van de zoektocht). Een chatfunctie, functioneel vergelijkbaar met WhatsApp, is eigenlijk ook heel logisch en zou in de basisfunctionaliteit kunnen zitten. Als er daarnaast meerwaarde is voor direct-messaging (één-op-één tussen zoekers) kun je dat als optionele functie kunnen zien, waarvoor zoekers de keuze hebben om wel of geen toestemming te geven.
Het uploaden van een "pasfoto" kan een vrije keuze van de gebruiker zijn.
Je eigen locatie zichtbaar maken voor de andere zoekers zou optioneel moeten zijn.
Stel je voor dat na installatie en voor het eerste gebruik van de app de gebruiker een aantal toestemmingsvinkjes kan plaatsen:

- Basisfunctionaliteit (noodzakelijk, anders is de app niet functioneel)
- Optionele functies (niet verplicht)

Gegevens verzamelen voor algoritmes te leren

4. Om beter een zoekgebied te kunnen bepalen, zouden we graag aanvullende gegevens willen. Bijvoorbeeld of iemand suïcidaal is, vaker is weggelopen, autistisch of een andere beperking. Dit is erg relevant om te bepalen waar men moet gaan zoeken. We kunnen deze gegevens mogelijk ook depersonaliseren na de zoekactie. Hoe zie jij dit?
5. Kunnen we deze (gedepersonaliseerde) gegevens ook gebruiken voor extern onderzoek en publicaties?

Dit is een lastige. Je gaat hiermee wel zeer gevoelige persoonsgegevens verwerken, tegelijkertijd bestaat er mogelijk wel een belangrijke meerwaarde bij het gebruik van deze gegevens. In geval van een minderjarige vermiste of een slachtoffer van een ongeval of misdrijf kan dit wel binnen de gekozen grondslag. In het geval van een vrijwillig vertrokken persoon wordt de onrechtmatige inbreuk op de persoonlijke levenssfeer nog groter en ernstiger.
Is het een optie om deze vragen met de coördinator mondeling door te nemen? Dan ben je namelijk niet aan het verwerken volgens de AVG.
Wellicht moeten we dit dilemma als gespreksonderwerp noteren voor de Autoriteit Persoonsgegevens.
Het verder verwerken van deze gegevens kan, mits je kunt garanderen dat die gegevens niet herleidbaar zijn naar een individu, zeker als deze nog in leven is. Voor overleden personen geldt de AVG niet en bestaat meer ruimte om persoonsgegevens te verwerken. Uit respect kan er echter voor gekozen worden deze gegevens ook te anonimiseren.

Gegevens vagen om algoritmes toe te passen

6. We zouden de gegevens in vraag 4 (bijv. suïcidaal) uiteindelijk ook willen gebruiken om een zoekgebied te bepalen. Kunnen we dit vragen?

WPG

7. Wat voor impact/beperkingen heeft de WPG voor ons platform?
8. Moeten/kunnen we onderscheid maken tussen algemene ondersteuning (geen expliciete Politietaak) en coördinatie (wel een Politietaak)? Zijn alle activiteiten van de Politie ook per definitie Politietaken, zoals beschreven in het WPG. Dit is mijns inziens niet helder beschreven waardoor het meekijken door de Politie niet onder WPG zou vallen.
9. Wanneer het dossier “overgedragen” wordt aan de Politie, vallen alle relevante gegevens onder WPG. Mogen wij deze dan nog muteren, aanvullen en delen?

Strikt genomen hoef je geen rekening te houden met de Wet politiegegevens, zolang de politie niet als verantwoordelijke optreedt voor de verwerking.
Politiegegevens zijn persoonsgegevens, verwerkt in het kader van de uitvoering van de politietaak. En de politietaak is in de Politiewet gedefinieerd als volgt: “De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.”
Aan de verwerking van politiegegevens zijn strikte eisen gesteld, bijvoorbeeld dat deze afgeschermd zijn voor onbevoegde personen. De politie is verantwoordelijk voor het nemen van maatregelen ter afscherming van politiegegevens tegen gebruik door onbevoegden. De politie zal nooit accepteren dat burgers met politiegegevens aan de slag gaan.
Zo bezien zijn de gegevens binnen de applicatie niet aan te merken als politiegegevens. De gegevens worden immers niet verwerkt door bevoegde personen en ook niet in het kader van het uitvoeren van de politietaak. De gegevens worden pas politiegegevens als (een kopie van) deze zijn opgenomen in het politiesysteem of -dossier. Maar ook dan zijn de (originele) gegevens in de app nog steeds

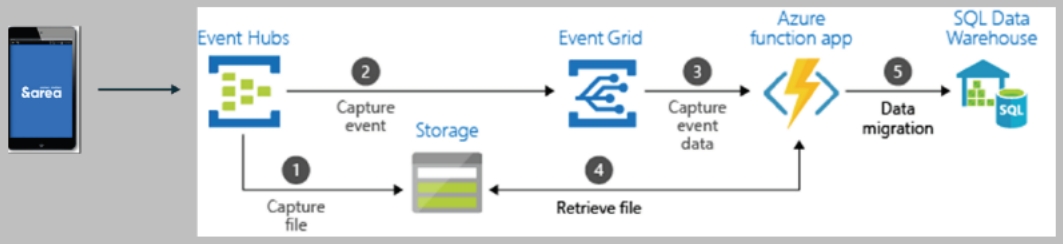
geen politiegegevens. De politie kan natuurlijk wel in het belang van het onderzoek vorderen dat verdere verwerking binnen de app wordt gestaakt. Of zelfs in het uiterste geval beslag leggen op de gegevens. Maar in een normale samenwerking met de politie bestaan er dus in een casus twee soorten persoonsgegevens naast elkaar:

- Persoonsgegevens in de app, onder verantwoordelijkheid van de aanbieder van de app;
- Politiegegevens in de politiesystemen, onder verantwoordelijkheid van de politie.

Per geval moet met de politie worden afgestemd welke gevolgstappen passend zijn.

8 ARCHITECTUUR

Todo: uitleg Maikel



8.1 GEADVISEERDE TECHNIEKEN

Content website

- CMS: 10.2.g

Web portalen

- Front-end: 10.2.g
- Back-end: 10.2.g
- Communicatie: 10.2.g

Mobile apps

- Front-end: 10.2.g
- Back-end: 10.2.g
- Communicatie: 10.2.g

Hosting

- 10.2.g, in Nederland

24x7 Beschikbaarheid

- D.m.v. 10.2.g

9 VOORSTEL REALISATIE

9.1 BEGROTING

9.1.1 ONTWIKKELING

Voor de ontwikkeling geldt een begrote ureninzet conform onderstaande tabel.

10 2.g

Uitgangspunten

- 100% must-haves
- 50% should-haves
- Inclusief beheerdocumentatie
- Inclusief licenties
- Inclusief overdracht naar beheer
- Exclusief vertaling EN: +/- € 10.2.g
- Exclusief afstemmen Autoriteit Persoonsgegevens
- Fixed budget (scrum)
- Uurtarief: € 10.2.g

Activiteit	Aantal	Tarief	Bedrag
Ontwikkeling	3.016 uur	€ 10.2.g	€ 10.2.g
Hosting OTAP-omgevingen	6 maanden	€ 10.2.g	€ 10.2.g
Totaal kosten van ontwikkeling			**€** 10.2.g

9.1.2 BEHEER

Hieronder staat een overzicht met indicatieve beheerkosten.

Activiteit	Maandelijks
Hosting (OTAP)	€ 10.2.g
Infra beheer (24x7)	€
Applicatiebeheer	€
Servicedesk*	€
Kaart abonnement*	€
Geografisch objecten abonnement*	€
Totaal	**€**

** Afhankelijk van het platform gebruik*

Applicatiebeheer

O.b.v. 22% van ontwikkelkosten per jaar, inclusief:

- Correctief onderhoud
- Preventief onderhoud
- Adaptief onderhoud

Exclusief:

- Additief onderhoud (nieuwe wensen)

Uitgangspunten

Inclusief:

- Hosting + failover
- Support
- Servicemanagement
- Abonnementen/ licenties
- Inclusief setup SLA

9.2 PLANNING

9.2.1 STROKENPLANNING

Onderstaande tabel geeft de planning weer in weken van de verschillende onderdelen van de realisatie van het platform.

10 2.g

9.3 VERVOLGSTAPPEN

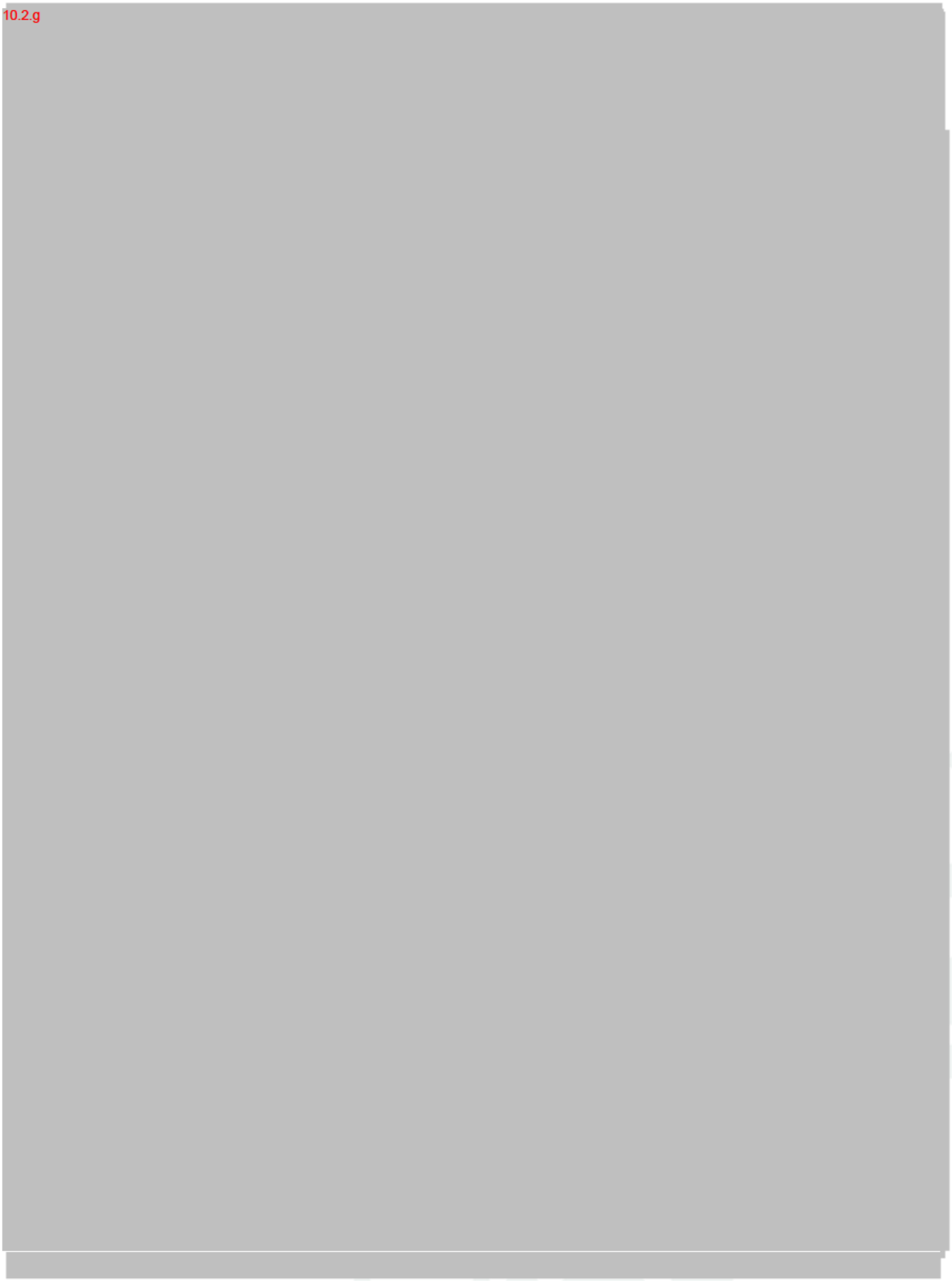
Todo

BIJLAGE A: FUNCTIONELE EISEN

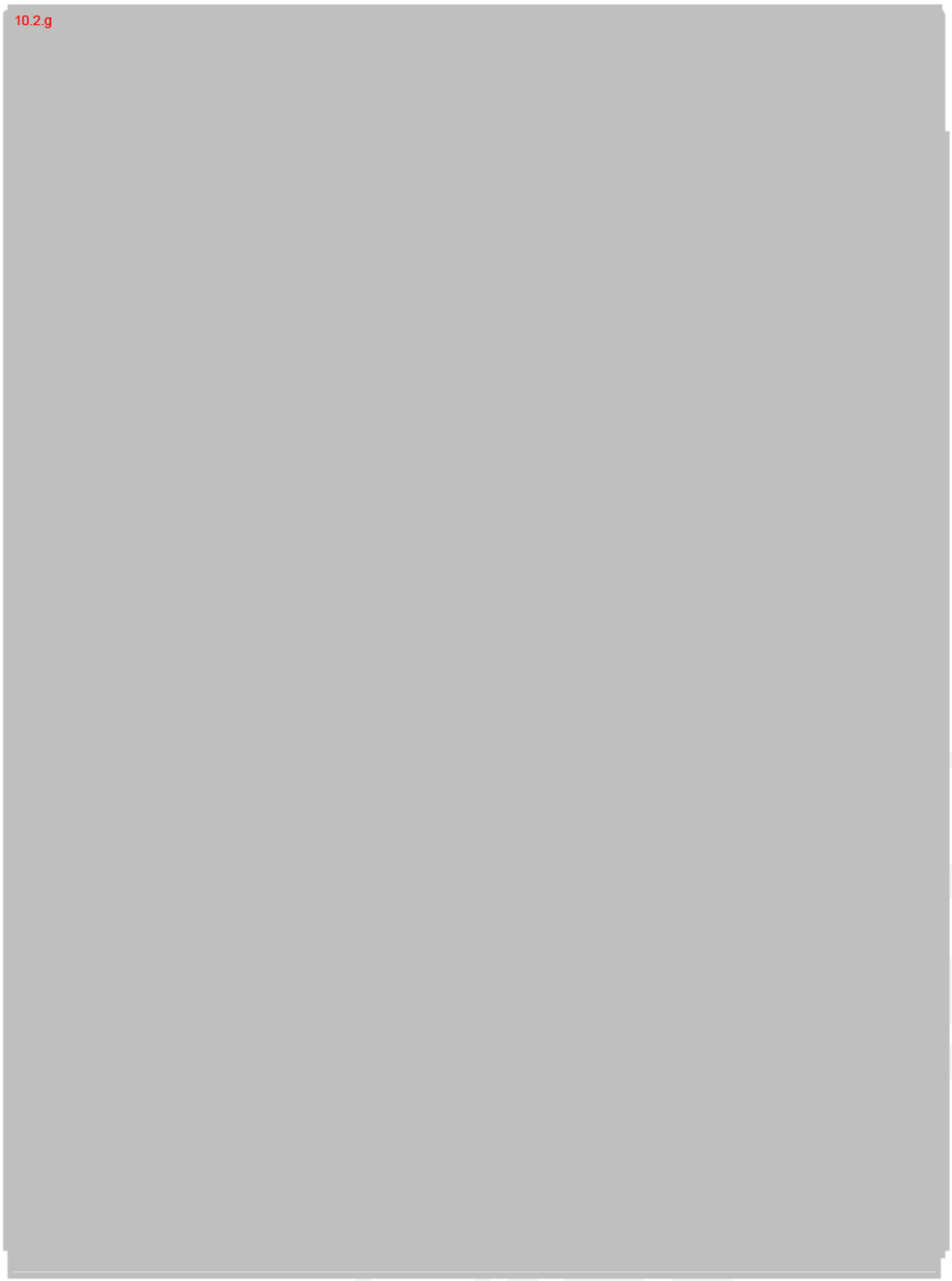
Zie ook Functionele Requirements v1.0.xlsx

10.2.g

10.2.g

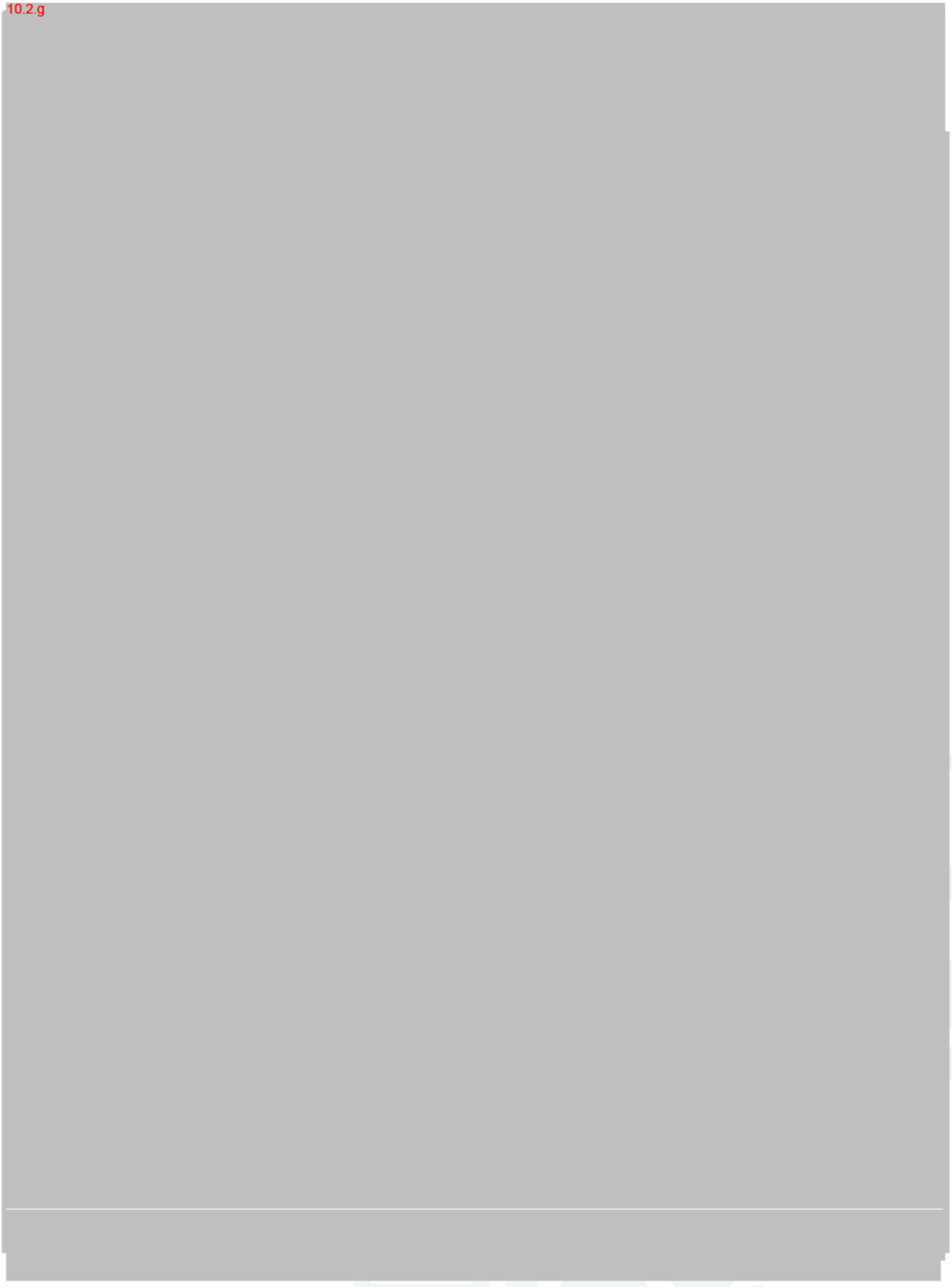


10.2.g



10.2.g

10.2.g



BIJLAGE B: NIET-FUNCTIONELE EISEN

ID	Hoofdcategorie	Subcategorie	Requirement	Prioriteit
10.2.g				

10.2.g