# BART! Ethiek, Privacy en Dataprotectie

## Functionele eisen en toekomstperspectief

Exemplaar Februari 2020 versie 0.9

**Auteurs:** Hans Arnold (TIGNL) en Jorrit van der Wal (CGI)

**Reviewers**: Mr. John Dijkers en Mr. Peter Tazelaar


Ministerie van Binnenlandse Zaken en Koninkrijksrelaties · POLITIE · Den Haag · TNO · Technology Investment Group · CGI · TU Delft

## Inhoudsopgave



Status exemplaar februari 2020 versie 0.9, redactie, lay-out en opmaak onderhanden werk nog niet definitief afgerond.

# 1. Management Samenvatting

Door BART! (Burger Alert Real Time) kunnen deelnemers in veiligheid- en leefbaarheidssystemen snel en gemakkelijk samen overlast tegengaan of oplossen. In geval van meer ernstige vormen van overlast of nood kunnen burgers een beroep doen op de overheid. Het gaat hierbij dan om het waarschuwen van de overheid, een helpende hand vragen of een spoed- melding van een incident doorgeven waarbij de hulp van overheid vereist is. Omgekeerd kan met BART! de overheid ook een beroep op burgers doen en hen handelings-perspectieven aanreiken. Op deze wijze kunnen burgers en overheden samenwerken om de leefbaarheid en veiligheid in de buurt te vergroten.

“Ethische, Privacy en Databescherming richtlijnen” zijn hierbij van cruciaal belang om de risico's en gevaren die het co-creëren van een veilige en leefbare buurt met zich meebrengt, te ondervangen. Binnen BART! zal rekening gehouden moeten worden met doelgerichtheid, proportionaliteit, subsidiariteit en tijdelijkheid. Niet elke veiligheidsbehoefte vergt vergaande inbreuken op de privacy en niet iedere inbreuk is toegestaan. Steeds moet de vraag worden gesteld of de maatregel niet te zwaar is met het oog op het gestelde doel en of er niet een ander, minder zwaar middel is waarmee hetzelfde doel kan worden bereikt. Voor de handhaving van de rechtsorde is het nodig dat noodzakelijke gegevens kunnen worden verzameld en op een betrouwbare, efficiënte en effectieve manie. Om vervolgens door middel van analyse en verwerking deze om te zetten in handelingsperspectieven voor burgers en professionals.

Op basis van kernwaarden gedefinieerd voor Burgers, Professionals en Technologie, kan BART! als participatiesysteem opgedeeld worden in drie interacterende deelsystemen, te weten:

1. Het “deelsysteem burgers” waarin burgers informatie via leefbaarheids- en veiligheidsapplicaties met elkaar en met de overheid kunnen delen en ook de toestemming van burgers voor het gebruik van de door hen aangereikte informatie is geregeld.
2. Het “deelsysteem Professionals”, waar de gegevens verwerkt worden tot handelings-perspectieven.
3. Het “deelsysteem Technologie“, het ondersteunde technische systeem dat op de achtergrond de communicatie tussen burgers en professionals afhandelt.

Deze opdeling vormt dan ook het raamwerk van kaders die gelden voor de functionele en technische specificaties, opgesteld vanuit het aandachtsgebied ”Ethiek, Privacy & DataProtectie (EP&DP)”.

Doelbinding, proportionaliteit, subsidiariteit en tijdelijkheid zijn belangrijke toetsingscriteria bij het verwerken van persoonsgegevens. Hierbij moeten de bijbehorende datastromen en processen zorgvuldig ingericht worden om overbodig gebruik van persoonsgegevens uit te sluiten. Om overbodige persoonsgegevens uit te sluiten zijn barrières nodig die zowel technisch, sociaal als organisatorisch van aard kunnen zijn. De barrières moeten over het gehele proces worden gepositioneerd om gezamenlijk een barrièremodel te vormen. In dit document worden een aantal barrières per domein beschreven. De barrières zijn van toepassing op de verschillende domeinen, omdat BART! veel verantwoordelijkheden bij burgers en professionals legt. De technologie kan uitkomsten bieden door burgers en professionals te ondersteunen.

# 2. BART! Ethiek, Privacy en Dataprotectie

In het project BART![1] werken politie, gemeente Den Haag, CGI, TNO, TIGNL en burgers samen. Het project BART! onderzoekt de mogelijkheden en vereisten voor een innovatief participatieconcept. Het concept ondersteunt de burger in het werken aan een veilige en leefbare buurt, samen met gemeente en politie. Zo bevorderen we de samenredzaamheid van buurten.

Binnen de co-creatie context 'het samen creëren van een leefbare en veilige samenleving', staat gelijkwaardigheid tussen burgers en de overheid voorop. Hierbij wordt verondersteld dat acties met betrekking tot het herstellen van overlast in wisselwerking tussen burger en overheid op maat tot stand komen. Door co-creatie tussen buurtbewoners en professionals kunnen leefbaarheid en veiligheidsinterventies beter aansluiten bij de behoefte en de dynamiek van een buurt.
Door BART! kunnen deelnemers in veiligheid- en leefbaarheidssystemen snel en gemakkelijk samen overlast of zonder hulp van de overheid herstellen. In geval van meer ernstigere vormen van overlast of nood kunnen burgers een beroep doen op de overheid. Het gaat hierbij dan om het waarschuwen van de overheid, een helpende hand te vragen of een spoed- melding van een incident door te geven waarbij de hulp van de overheid vereist is. Omgekeerd kan met BART! de overheid ook een beroep op burgers doen en hen handelingsperspectieven aanreiken.  Op deze wijze kunnen burgers en overheden samenwerken om de leefbaarheid en veiligheid in de buurt te vergroten.

## 2.1 Ethische aspecten BART!

De samenleving zijn wij allen tezamen, wijzelf, onze buren, onze familie, onze vrienden, alle mensen in onze nabije omgeving in de buurt, de wijk, stad etc.  De samenleving verlangt van ons dat wij samen zorg dragen voor een leefbare en veilige stad, wijk of buurt. Binnen BART! betekent dit dat burgers, professionals, bedrijven, gemeenten en de politie samen op een effectieve wijze zorg dragen voor een leefbare en veilige stad, wijk of buurt. BART! werkt alleen als mensen het kunnen vertrouwen. Cruciaal voor dit vertrouwen is dat BART! integer is. Integer houdt in dat er sprake is van intrinsieke betrouwbaarheid. Dit betekent dat BART!’s functie en werking transparant beschreven is en overeenkomstig functioneert.

BART! dient dus integer te zijn en verbinding tot stand te brengen. Dit betekent dat BART! ethische richtlijnen volgt. Dit houdt in dat ervoor gezorgd is dat de gedragingen van BART! met betrekking tot het creëren van een veilige en leefbare samenleving bijdragen aan het verbeteren van wederzijdse betrokkenheid en vertrouwen tussen burgers, bedrijven, gemeente en politie.  BART! draagt hierdoor bij aan een veilige leefomgeving waarin kernwaarden zoals zelfbeschikking, vrijheid, naastenliefde, samenredzaamheid en rechtvaardigheid tot bloei kunnen komen en mensen zonder angst samen kunnen leven en werken. Het samen werken aan het welzijn van mensen is een belangrijk verbindend element.

[1] BART! - Burger Alert Real Time, https://www.bartportal.nl/

Welzijn hangt nauw samen met goed sociaal contact met de mensen om ons heen en dingen doen waardoor je iets voor iemand anders kan betekenen[2]. Mensen willen het gevoel hebben ergens bij te horen.[3]

Als we het over het beheersen van leefbaarheid en veiligheid hebben, dan hebben we het bij BART! over maatregelen voor de aanpak van problemen in de openbare ruimte, het bieden van noodhulp en het reduceren van criminaliteit. Veiligheid kan binnen BART! worden opgevat als een samenbundeling van het voorkomen of reduceren van risico's die een burger in het bestaan of functioneren kunnen bedreigen, die de 'normale toestand' aantasten.

Als burgers zich veilig voelen en vertrouwen hebben, durven zij zich in vrijheid te bewegen, zaken met elkaar te doen, samen te werken. Het gevoel veilig te zijn is ook een basale menselijke behoefte. Het waarborgen van privacy en veiligheid zijn basisvoorwaarden voor het functioneren van een burgerparticipatiesysteem als BART!, omdat dit één van de noodzakelijke voorwaarden is voor burgers om vertrouwen te kunnen hebben in het systeem.

Door BART! kunnen deelnemers in digitale buurtgroepen snel en gemakkelijk een beroep doen op de overheid in geval van overlast, nood, om hen te waarschuwen, een helpende hand te vragen of een spoedmelding van een incident door te geven waarbij de hulp van overheid vereist is. Omgekeerd kan met BART! de overheid ook een beroep op participanten doen en hen handelingsperspectieven aanreiken of vragen stellen. De betrokkene binnen BART! kan zijn een melder, verdachte, slachtoffer, wettelijk vertegenwoordiger of een hulpverlener.

BART! faciliteert daarmee de communicatie, welke het fundament is voor participatie. Doordat burgers en overheden beter informatie met elkaar uitwisselen kan er meer maatwerk worden geleverd en kan de overheid pro-actiever optreden.

In een gemeente zal de dienstverlening verbeteren, omdat gemeenten die diensten beter af kunnen stemmen op de burger. Voor de politie gaat BART! invloed hebben op een grotere heterdaadkracht en op de capaciteit en het effectief en efficiënt inzetten van beschikbare politiemensen.

## 2.2 Privacyaspecten BART!

Het doel van BART! is burgers en professionals in hun eigen kracht te ondersteunen en samen te werken aan samenredzaamheid ten behoeve van het verbeteren van een leefbare en veilige woonomgeving. Hiervoor werkt BART! met persoonsgegevens die alleen worden gebruikt om de doelstelling van BART! "samenredzaamheid ten behoeve van het verbeteren van een leefbare en veilige- woon- en werkomgeving" te bereiken. BART! maakt het voor professionals mogelijk om, snellere en betere dienstverlening te leveren. Daarbij vergroot het de saamhorigheid tussen

[2] https://www.gemeente.nu/bestuur/gemeenten-kunnen-geluk-beinvloeden/
[3] 'Erbij willen horen' werd in 1943 door Abraham Maslow op de derde plaats gezet van zijn bekende piramide van Maslow. Deze piramide geeft een ordening van universele behoeftes weer. Erbij willen horen komt onder zelfontplooiing en behoefte aan waardering en erkenning, maar boven behoefte aan veiligheid en zekerheid en lichamelijke behoeften.

wijkbewoners. Dit betekent dat burgers, professionals, bedrijven, gemeenten en de politie samen op een effectieve wijze zorg dragen voor een leefbare en veilige stad, wijk of buurt.

Overheidspartijen binnen BART! dragen op efficiënte en doelmatige wijze zorg voor een leefbare en veilige woonomgeving, voor de handhaving van de rechtsorde en het adequate afhandelen van overlastmeldingen. Het gaat concreet om het beschermen van personen of goederen, het begrenzen van ongewenst gedrag en het bekrachtigen van gewenst gedrag.

Voor de handhaving van de rechtsorde is het nodig dat noodzakelijke gegevens kunnen worden verzameld en op een betrouwbare, efficiënte en effectieve manier kunnen worden geanalyseerd, verwerkt en omgezet in handelingsperspectieven voor burgers en professionals[4]. Binnen het BART!-concept zijn overheidspartijen zoals een gemeente en de politie verwerkings- verantwoordelijke zoals gedefinieerd in de Algemene verordening gegevensbescherming (AVG) respectievelijk de Wet politiegegevens (Wpg)[5].

Informatie wordt verzameld, verwerkt, en gedeeld wanneer dit noodzakelijk is voor het treffen van maatregelen voor het beheersen van overlast, het bieden van noodhulp en het reduceren van criminaliteit en het herstellen van de rechtsorde.

Overlastmeldingen kennen bepaalde gradaties waarbij voor de afhandeling van sommige overlastmeldingen geen persoonsgegevens nodig zijn en voor de afhandeling van andere meldingen deze wel nodig zijn. Indien gegevens over personen die zijn betrokken bij een incident een cruciale rol spelen om een overlastmelding af te handelen, heeft BART! te maken met geheimhouding en moet het verwerken van deze persoonsgegevens overeenkomstig de AVG of de Wpg plaatsvinden.

## 2.3 Ethiek en privacy in evenwicht

Betrokken personen moeten erop kunnen vertrouwen dat bij de snelle en goede hulpverlening de medewerkers op de meldkamers van de politie of Klant Contact Centrum (KCC) van de gemeente van de gemeente zorgvuldig omgaan met persoonsgegevens. Tegelijkertijd spelen andere belangen een rol zoals de spoedige afhandeling van een melding en de veiligheid van burgers en hulpverleners. De privacywetgeving , de AVG en de Wpg, gaan uit van de verantwoordelijkheid voor de gegevensverwerkingen en verlangt dat allen die toegang hebben tot de gegevens aan geheimhouding zijn gebonden.[6]

Samenwerking van professionals vereist eenduidige handelingsperspectieven gebaseerd op zingeving en klantgerichte dienstverlening voor iedere betrokkene in de keten, met toetsbare verantwoording achteraf. Zingeving, ethisch en oprecht handelen is onlosmakelijk verbonden met het werken in het leefbaarheids- en veiligheidsdomein. Zingeving, ethisch en oprecht handelen vanuit het alledaags

[4] EP&DP Principe 33, zie Publicatie Ethiek & Privacy By Design ISBN/EAN no.: 978-90-829873-0-0
[5] https://wetten.overheid.nl/BWBR0040940/2019-02-19
[6] EP&D Principe 34, zie Publicatie Ethiek & Privacy By Design ISBN/EAN no.: 978-90-829873-0-0

professionele perspectief kan hierbij worden bereikt door: te handelen op basis van principiële principes, doelen te stellen, zelfbeheersing, verdieping in andermans denken, de mogelijkheden en beperkingen van het systeem te kennen, verbinding te maken met hogere doelen en te trachten beter te presteren dan voor mogelijk gehouden is. Deze onderwerpen dienen binnen betrokken organisaties gewaarborgd te worden in onder andere communicatie, governance, processen, uitvoering, opleidingen, beroepstrainingen en beleidsontwikkeling.

# 3. Ethische en Wettelijke kaders

Voor de handhaving van de rechtsorde is het nodig dat noodzakelijke gegevens kunnen worden verzameld en op een betrouwbare, efficiënte en effectieve manier. Deze gegevens moeten geanalyseerd, verwerkt en omgezet kunnen worden in handelingsperspectieven voor burgers en professionals.[7]

Ethische, Privacy en Databescherming richtlijnen zijn hierbij van cruciaal belang om de risico's en gevaren die het co-creëren van een veilige en leefbare buurt met zich meebrengt, te ondervangen. Niet elke veiligheidsbehoefte vergt vergaande inbreuken op de privacy en niet iedere inbreuk is toegestaan. Steeds moet de vraag worden gesteld of de maatregel niet te zwaar is met het oog op het gestelde doel (proportionaliteit) en of er niet een ander minder zwaar middel is waarmee hetzelfde doel kan worden bereikt (subsidiariteit). Dit moet gemotiveerd kunnen worden op basis van vooraf vastgesteld beleid.[8]

Privacy kan verbijzonderd worden in relationele privacy en informationele privacy. Relationele privacy heeft betrekking op de persoonlijke levenssfeer, het recht op individuele vrijheid, rust om tot authenticiteit te komen en het recht om zich te beschermen tegen handelingen of beslissingen die van invloed zijn op de levensomstandigheden. De vraag hierbij is vervolgens tot waar die persoonlijke levenssfeer zich uitstrekt, wat de beschermwaardigheid van dat bereik is en wie invloed heeft op andermans privacy. Informationele privacy gaat over de bescherming tegen ongerechtvaardigde verwerking van persoonsgegevens. [9]

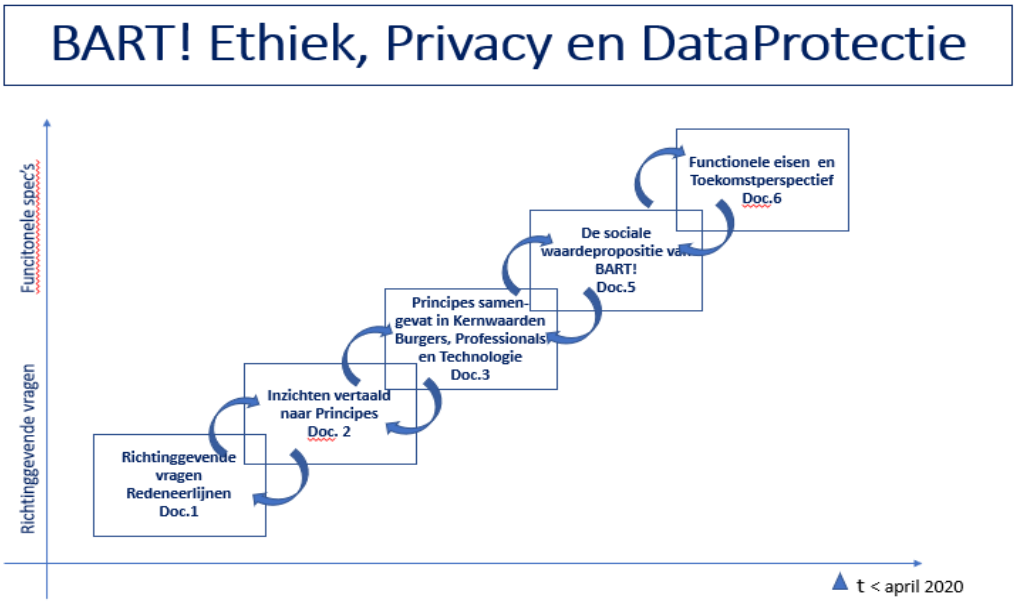
Tot slot, er zijn enkele belangrijke wetten die de ontwerpeisen van BART! op het gebied van Ethiek, Privacy en DataProtectie (EP&DP) vormgeven. De Algemene verordening gegevensbescherming van de Europese Unie stelt regels over het gebruik van persoonsgegevens en het beschermen daarvan. Binnen BART! staat de AVG niet op zichzelf. Betreffende het veiligheidsdomein zijn ook andere wetten van kracht die in samenhang moeten worden bezien en gewogen in het kader van het te bereiken veiligheidsdoel.

[7] https://wetten.overheid.nl/BWBR0022463/2019-01-01
[8] EP&DP Principe 22, zie Publicatie Ethiek & Privacy By Design ISBN/EAN no.: 978-90-829873-0-0
[9] Privacyregulering-in-theorie-en-praktijk-j.m.a.-berkvens

De bescherming van persoonsgegevens bij de politie is geregeld in de Wet politiegegevens (Wpg), die gebaseerd is op een Europese richtlijn voor wethandhavingsorganisaties en autoriteiten. De Wpg regelt de verwerking van politiegegevens door de Nationale Politie, de Koninklijke marechaussee, de Rijksrecherche, de bijzondere opsporingsdiensten en de buitengewone opsporingsambtenaren.

# 4. Kernwaarden Burgers, Professionals en Technologie

Op basis van antwoorden op geformuleerde richtinggevende onderzoeksvragen zijn een aantal principes geformuleerd. Deze principes zijn vervolgens gebundeld in onderstaande gedefinieerde kernwaarden geldend voor Burgers, Professionals en Technologie.




Na het benoemen en toelichten van de kernwaarden volgt een analyse over toekomstperspectieven waarin de onderstaande kernwaarden terugkomen.

## 4.1 Kernwaarden BART! voor burgers in het bijzonder

1. **Burgers die deelnemen in digitale buurtgroepen en overlast melden via social media.**
   Burgers in digitale buurtgroepen verzamelen en delen alleen informatie wanneer dit noodzakelijk is voor het treffen van maatregelen voor:
   i. het bieden van hulp
   ii. het beheersen van overlast
   iii. het voorkomen of bestrijden van criminaliteit

2. **Tussen burgers en overheden is vastgesteld welke soort informatie verzameld en gemeld wordt.**
   Burgers die deelnemen in digitale buurtgroepen geven overlast, verdachte situaties of gepleegde wetsovertredingen door aan overheidsorganisaties. Burgers hebben met betrekking tot doelbinding en minimale gegevensverwerking met de overheid afgestemd welke soort informatie verzameld en gemeld wordt om de gegevensuitwisseling te stroomlijnen en doelmatig te houden.[10]

3. **Burgers melden volgens een met de overheid afgestemde procedure**
   Burgers die deelnemen in digitale buurtgroepen melden volgens een met de overheid afgestemde procedure.

4. **Burgers in buurtgroepen en ondersteuning overheid**
   Burgers in digitale buurtgroepen kunnen, indien zij dat wensen, op het vlak van competentie, advies en ontwikkeling, online ondersteund worden door de (lokale) overheid.

5. **Burgers in buurtgroepen bewaken en respecteren bewust persoonsgegevens**
   Burgers moeten zich bewust zijn van de waarde van hun persoonsgegevens en deze én die van anderen bewaken en eerbiedigen. Aldus, burgers maken persoonsgegevens van anderen niet openbaar (rechtmatigheid[11]). Om die reden moet de burger bij meldingen in beginsel vermijden personen en/of situaties te beschrijven waarbij personen herleidbaar zijn. De burger mag niet zomaar beelden/opnames van gezichten, kentekens, herkenbare locaties, binnen woningen en herkenbaar stemgeluid delen.

6. **BART!-meldingen bevatten geen opmerkingen die beledigen bevatten, die bedreigen of aanzetten tot geweld of andere vormen van eigenrichting**
   Burgers in digitale buurtgroepen houden zich aan de wet. Dit betekent dat bij het melden van overlast via social media melders elkaar niet mogen aanzetten tot haat of geweld of andere mensen mogen beledigen. Ook mogen geen uitingen gedaan worden waardoor iemand zich bedreigd, gediscrimineerd of onveilig kan voelen vanwege ras, herkomst, geloof, geaardheid of leefstijl die hij of zij heeft.

7. **Melding overlast en verdachte situatie die een directe bedreiging van de leefomgeving vormen**
   Indien het gaat om meldingen van overlast, verdachte situaties of geconstateerde feiten die een directe bedreiging van de leefomgeving vormen, mogen deze meldingen wel beelden of beschrijvingen bevatten die mogelijk een inbreuk maken op de privacy van (alleen) de betrokken persoon/personen. Dergelijke privacygevoelige meldingen worden uitsluitend bij de politie gemeld. De overige deelnemers in de buurtgroep kunnen op de hoogte worden gebracht met een melding die deze privacygevoelige informatie niet bevat.

[10] Art. 5, lid 1, sub b/c AVG en art. 3 Wpg
[11] Art. 5, lid 1, sub a AVG

8. **Burgers melden overlast zonder inbreuk te maken op iemands privacy**
   In een melding kunnen burgers zonder inbreuk te maken op iemands privacy wel het geslacht, de geschatte leeftijd en iemands lengte, postuur, haarkleur en kapsel, kleding, bagage en het merk, kleur en model van een auto in een melding opnemen.

9. **Burgers mogen nooit voor eigen rechter spelen of geweld gebruiken om overlastsituaties te stoppen**
   Burgers mogen nooit voor eigen rechter spelen of geweld gebruiken om overlastsituaties te stoppen of om in te grijpen bij het plaatsvinden van strafbare feiten, tenzij er sprake is van zelfverdediging of noodweer. Wacht na een melding bij de politie de komst van de politie af.

10. **Burgers en onrechtmatig gebruik van persoonsgegevens**
    Burgers die vinden dat hun persoonsgegevens niet volgens deze kernwaarden op social media geplaatst zijn, kunnen daarover een klacht indienen bij de beheerder van de applicatie die zij gebruiken om meldingen door te geven. Deze beheerder kan vervolgens actie ondernemen om het bericht te verwijderen. Daarnaast is de overheidsorganisatie die het bericht geplaatst heeft verantwoordelijk voor de verwerking. Een klachtenprocedure kan worden gestart bij de desbetreffende organisatie of de Autoriteit Persoonsgegevens.

## 4.2 Kernwaarden BART! professionals in het bijzonder

1. **BART! professionals beschikken over afspraken m.b.t. privacy inbreuk makende maatregelen:**
   1) Ze hebben afspraken tot hun beschikking tot wanneer op de privacy inbreuk makende maatregelen kunnen worden toegepast. Belangrijk hierbij is dat bij de verwerking van persoonsgegevens de privacy van de betrokkene en eventuele derden zo min mogelijk geschaad mag worden. Een proportionaliteit- en subsidiariteitsmatrix biedt hierbij een helpende hand. Hieronder valt ook de verwerkingsgrondslag op basis van toestemming van de burger aan de hand van een privacyverklaring.[12]
   2) Ze werken alleen met persoonsgegevens wanneer het doel specifiek omschreven en vastgesteld is. Wanneer persoonsgegevens voor een ander doel worden verwerkt, is vastgesteld of het nieuwe doel verenigbaar is met het oorspronkelijke doel (doelbinding[13]).
   3) Ze kunnen handelingsperspectieven, gemaakte keuzes en verrichte handelingen altijd achteraf verantwoorden (transparante en behoorlijke verwerking[14]).

[12] Art. 6 AVG
[13] Art. 5, lid 1, sub b AVG en art. 3 Wpg
[14] Art. 5, lid 1, sub a AVG

2. **In BART! worden handelingsperspectieven verstrekt aan:**
   1) Burgers: personen zoals slachtoffers en verdachten, zijn in principe niet herkenbaar of herleidbaar in beeld. De overheid zal in beginsel geen herkenbare beelden van slachtoffers of verdachten ter beschikking stellen aan burgers. Alleen de politie mag dat doen nadat het OM de politie via interne processen hiervoor toestemming heeft gegeven;
   2) Professionals kunnen altijd over beelden beschikken die herkenbaar en herleidbaar zijn;

3. **BART! professionals en gegevens vernietigen of geanonimiseerd hergebruiken**
   Persoonsgegevens moeten op enig moment worden vernietigd. De AVG stelt dat er redelijke bewaartermijnen moeten worden bepaald en de Wpg geeft vaste bewaartermijnen. Omtrent vernietiging is het belangrijk dat professionals gegevens vernietigen wanneer dit moet volgens de afgesproken bewaartermijn. Partijen die vallen onder de AVG moeten dus zelf bewaartermijnen bepalen, rekening houdend met doelbinding en de eis van minimale gegevensverwerking.[15] Zodra gegevens niet meer noodzakelijk zijn moet de partij deze vernietigen om ongeoorloofde 'bulking' te voorkomen. Bulking staat hier voor het verzamelen en stapelen van steeds grotere hoeveelheid data.

   Voor de politie is de Wpg van toepassing die onderscheid maakt tussen verwijderen en vernietigen.[16] Zodra BART!-data bij de politie binnenkomt valt deze data onder de Wpg, waar gegevens niet direct vernietigd worden. Na het aflopen van de termijn die geldt voor het gebruik ten behoeve van de uitvoering van de politietaak maakt de politie de gegevens ontoegankelijk voor de uitvoering van de politietaak (verwijderen), waarna deze later (afhankelijk van beoordeling noodzaak en bewaartermijnen) moeten worden vernietigd. De Officier van Justitie kan verwijderende gegevens toegankelijk maken indien dit noodzakelijk is ten behoeve van een opsporingsonderzoek.

   Nadat gegevens geanonimiseerd zijn kunnen deze door de professional worden gebruikt voor onderzoeksdoeleinden zoals trendanalyses over een buurt. In dat geval bewaar je enkel het label van de melding, bijvoorbeeld afval op straat of diefstal, en koppel je dat aan een geografische locatie. In dat geval zijn AVG en Wpg niet meer van toepassing, omdat er geen persoonsgegevens meer worden verwerkt.

4. **BART! en Rechten van de betrokkene**
   'Rechten van de betrokkene' is een belangrijke pijler binnen de AVG[17] en Wpg[18] voor het waarborgen van de privacy van de burger en past binnen het streven van de overheid om transparant te zijn richting de maatschappij. Dit recht biedt de burger namelijk de mogelijkheid informatie te verkrijgen over de gegevens die een BART!-ketenpartner over

[15] Art. 5, lid 1, sub c AVG
[16] Art. 14 Wpg
[17] Art. 12 tot en met art. 23 AVG
[18] Art. 24a tot en met art. 28 Wpg

hem of haar heeft opgeslagen (recht op inzage) en die ketenpartner te verzoeken deze te corrigeren of te verwijderen indien de gegevens onjuist zijn.

Als betrokkene van mening is dat de gegevens niet kloppen, dan kan betrokkene een schriftelijk verzoek bij de betreffende BART! professional indienen waarin wordt aangeven wat er gewijzigd moet worden. BART! professionals hebben het recht een verzoek om inzage, correctie of verwijdering af te wijzen onder andere als de veiligheid in het geding is of als het een ongegrond of buitensporig verzoek is (de weigeringsgronden van AVG en Wpg zijn onderling enigszins verschillend).

Het op de hoogte stellen van betrokkenen (de informatieplicht op grond van de AVG) moet zowel bij het verwerken van gegevens met toestemming (de melder) als verwerking van gegevens zonder toestemming (de persoon over wie gemeld wordt). Bij BART! zijn beide belangrijk, omdat meldingen persoonsgegevens van anderen dan de melder kunnen bevatten.

De overheidspartijen die persoonsgegevens verwerken op basis van de AVG hebben namelijk de plicht om de betrokkenen op de hoogte te stellen, indien dit onmogelijk of onevenredig is mag dit ook publiekelijk door informatie openbaar te maken. Overheden dienen hier zorgvuldig mee om te gaan. Persoonsgegevens die niet noodzakelijk of doelmatig zijn dienen daarom zo spoedig mogelijk te worden vernietigd.

Inzake rechten van betrokkenen bestaat een principieel onderscheid tussen gegevens die de politie verwerkt overeenkomstig de Wpg enerzijds en de verwerkers van de gemeente die vallen onder de AVG anderzijds. Met betrekking tot gegevens over een verdachte heeft de politie minder dwingende informatieplicht en ruimere mogelijkheden om een verzoek om inzage te weigeren. Dit is anders bij de gemeente die verwekingen doen onder de AVG waarbij in beginsel wel informatieplicht geldt, maar de gemeente minder mogelijkheden heeft om een verzoek om inzage te weigeren.

5. **BART! professionals kunnen gebruik nieuwe BART!-technologie uitleggen**
De internationale principes van mensenrechten geven het kader aan waarbinnen overheidsorganisaties en professionals algoritmes kunnen ontwikkelen.

Dit houdt in dat algoritmes binnen BART! de gelijkwaardigheid en autonomie van individuen moeten respecteren en zich houden aan de universele rechten van de mens en zich tevens houden aan de wet (AVG, Wpg en WvSv) met bijbehorende (bestuurlijke) verantwoordelijkheid.

Professionals gebruiken om die redenen alleen algoritme-gedreven technologieën en nieuwe media die zo ontworpen zijn dat deze de gelijkheid en autonomie van individuen respecteren én zich houden aan het recht op leven, privacy, religie, eigendom, vrijheid van denken. Ze maken alleen gebruik van artificiële intelligentie, big-data analyses en slimme algoritmes, die vooraf transparant en eenvoudig uitlegbaar zijn. Ze beoordelen voorafgaand aan het gebruik van nieuwe media en technologie of deze ‘zo gericht mogelijk’ wordt ingezet en of er niet

minder vergaande manieren voorhanden zijn om aan de gewenste informatie te komen (proportionaliteit/subsidiariteit). De overheidsorganisaties dienen de inzet van nieuwe technologie eenvoudig te kunnen motiveren en verantwoorden. Dit wil zeggen dat transparantie uiterst belangrijk is. Zonder transparantie is er sprake van een zogenaamde 'blackbox', een systeem dat niet te volgen of te doorgronden is. De gewenste situatie is een doorzicht systeem (glass box), waardoor professionals inzicht hebben en grip krijgen op de geleverde informatie.

6. **BART! Professionals en logging gebruik van gegevens**
   Alleen BART! professionals die daartoe geautoriseerd zijn krijgen toegang tot gegevens.[19] Binnen de AVG valt autorisatie onder de veelgenoemde technische en organisatorische waarborgen voor gegevensbescherming. Zij mogen alleen die gegevens inzien die zij nodig hebben om hun taak uit te voeren.

   Bijgehouden (gelogd) dient te worden wie welke handeling op welk tijdstip uitvoert in een bepaald bestand. BART! professionals hebben passende maatregelen – technisch en organisatorisch – getroffen om persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking, tegen opzettelijk verlies, vernietiging of beschadiging. Dit betreffen veiligheidsmaatregelen zoals in de AVG staan omschreven met de bijbehorende logging om het gebruik van de systemen en bijbehorende data transparant te maken met als doel verantwoordelijk gedrag te borgen. Voor de politie is logging ook een eis die in de Wpg staat (en ook wel wordt uitgevoerd maar nog niet van kracht is).[20]

   Logging is van toepassing op het organisatorische gedeelte van BART!, namelijk het dashboard of andere vorm van (visuele) informatieverstrekking. De handelingen van de professional hierop zijn onderworpen aan logging. De handelingen van de technologie in de verwerkingsunit zijn niet onderworpen aan logging, omdat de professional hier geen invloed op heeft.

7. **Professionals hebben procedures om te acteren bij misbruik van BART!**
   Burgers kunnen misbruik maken van BART! door valse meldingen te doen of door meldingen in besloten groepen zoals digitale buurtgroepen te misbruiken. Procedures moeten professionals mogelijkheden geven om burgers die het proces verstoren uit te sluiten van BART!. Het gaat hier om een zogenaamde 'blacklist' die technisch geïmplementeerd moet worden.

[19] Art. 6 Wpg
[20] Art. 32 AVG en art. 32a Wpg

## 4.3 Kernwaarden voor de BART!-technologie in het bijzonder

1. **BART!-technologie, artificiële intelligentie, slimme algoritmes, data-analyses, machine learning**
   De internationale principes van mensenrechten geven het kader aan waarbinnen artificiële intelligentie, slimme algoritmes, data-analyses, machine learning etc. die binnen de BART! innovatieve technologie zijn opgenomen, gebruikt kunnen worden.

   Zoals bij kernwaarde vijf onder professionals is aangekaart mag deze technologie niet onevenredig mensenrechten beperken. Daarnaast moet AI in de breedste zin van het woord transparant zijn, zodat professionals de 'gedachtegang' van de technologie kunnen volgen. Op die manier ondersteunt de technologie in plaats van dat de technologie gaat dicteren en de mens slechts de uitkomsten opvolgt.

2. **BART! en rechtmatige wijze van verzamelen, verwerken informatie en hergebruik geanonimiseerde gegevens**
   Binnen BART! is technisch geborgd dat informatie op een rechtmatige wijze verzameld en verwerkt wordt waarbij de privacy van de betrokkene en eventuele derden zo min mogelijk geschaad wordt. De verwerkingsunit moet technische maatregelen bevatten ten behoeve van ethiek, privacy en dataprotectie. Hieronder valt het herkennen van persoonsgegevens waarop aansluitende acties volgen voor compliance met de AVG en Wpg.

   Gegevens binnen de technische verwerkingsunit worden vernietigd nadat deze zijn doorgestuurd naar de desbetreffende overheidspartij. In het kader van privacy en dataprotectie is het vereist dat de verwerking zodanig snel gaat (real time) dat de persoonsgegevens direct kunnen worden vernietigd binnen de verwerkingsunit.

   In het kader van rechten van betrokkenen kunnen burgers verzoeken om inzage en rectificatie indienen bij de overheidspartijen die hun persoonsgegevens verwerken. BART! zet de data uit meldingen enkel door op een snelle manier, waardoor het als doorgeefluik functioneert in plaats van als een database. Betrokkenen moeten op in beginsel op de hoogte worden gesteld van de verwerking. Echter, er zijn uitzonderingen voor de politie (Wpg) en overheidspartijen die op basis van de AVG persoonsgegevens verwerken.[21] Zodoende hoeft de politie geen informatie over de verwerking te verstrekken aan verdachten.

   BART! technologie is in staat verzamelde gegevens te anonimiseren voor hergebruik ten behoeve van anonieme trend-database met een visualisatie als extra functionaliteit. Op deze manier kunnen probleemwijken of risicovolle incidenten worden opgemerkt en kunnen preventieve/structurele maatregelen ontwikkeld worden die een meerwaarde vormen voor burgers en overheid.

[21] Art. 24b, lid 3 Wpg en art. 14, lid 5 AVG

3. **In BART!-meldingen zijn gebruikte persoonsgegevens permanent gebonden**
   In BART! meldingen zijn informatie en persoonsgegevens permanent technisch gebonden aan de originele context waarbinnen de melding gedaan is. Het gebruik van persoonsgegevens binnen BART! is technisch zo ingericht dat deze alleen maar gebruikt kunnen worden om het vooraf gestelde doel te bereiken (doelbinding).[22]

4. **BART! herkent misbruik in de vorm van valse meldingen**
   BART! moet in staat zijn om in bepaalde mate valse meldingen en misbruik te signaleren. Door professionals in te lichten over potentieel misbruik van BART! in de vorm van valse meldingen, kunnen acties worden ondernomen om de bron van het misbruik af te sluiten van BART!. Hierdoor kan bepaalde input worden geweerd, waardoor professionals op basis van kwalitatieve data kunnen handelen.

5. **BART! en het herkennen van beelden**
   Omdat BART! niet enkel gericht is op tekst, maar ook op beelden is het belangrijk dat de verwerkingsunit ook op dat gebied zaken kan herkennen. BART! moet in staat zijn om persoonsgegevens zoals kentekens en gezichten op beelden te onderkennen. Ten eerste om de professionals te signaleren en te ondersteunen. Ten tweede, verdere ontwikkeling van BART kan het mogelijk maken dat de technologie automatisch persoonsgegevens afschermt zoals het blurren van gezichten, alvorens de beelden worden meegegeven met de melding richting professionals.

6. **BART! automatisch gegenereerde geleerde lessen**
   BART! draagt er technisch zorg voor dat elk incident geregistreerd wordt en dat bijzonderheden ter ondersteuning of ter transparantie (verantwoording) worden gecommuniceerd met de professionals. Professionals moeten op hun beurt in staat zijn om meldingen ‘te flaggen’ om de verwerkingsunit (AI) verder te ontwikkelen. Flaggen is het duiden van een melding door aan te geven wat de verwerkingsunit over het hoofd heeft gezien. Kortweg, kan de professional foutcodes aangeven om het systeem te verbeteren.

7. **De technologie van BART! en het bijbehorende proces moeten veilig ingericht zijn**
   Technische en bijbehorende organisatorische maatregelen moeten genomen worden om een hoog securitylevel te borgen, waarmee de integriteit van BART! gewaarborgd blijft. Dit strekt van de beveiliging van databases en de encryptie van data tot aan het nemen van maatregelen ter bevordering van de betrouwbaarheid van het menselijk handelen, bijvoorbeeld screening.

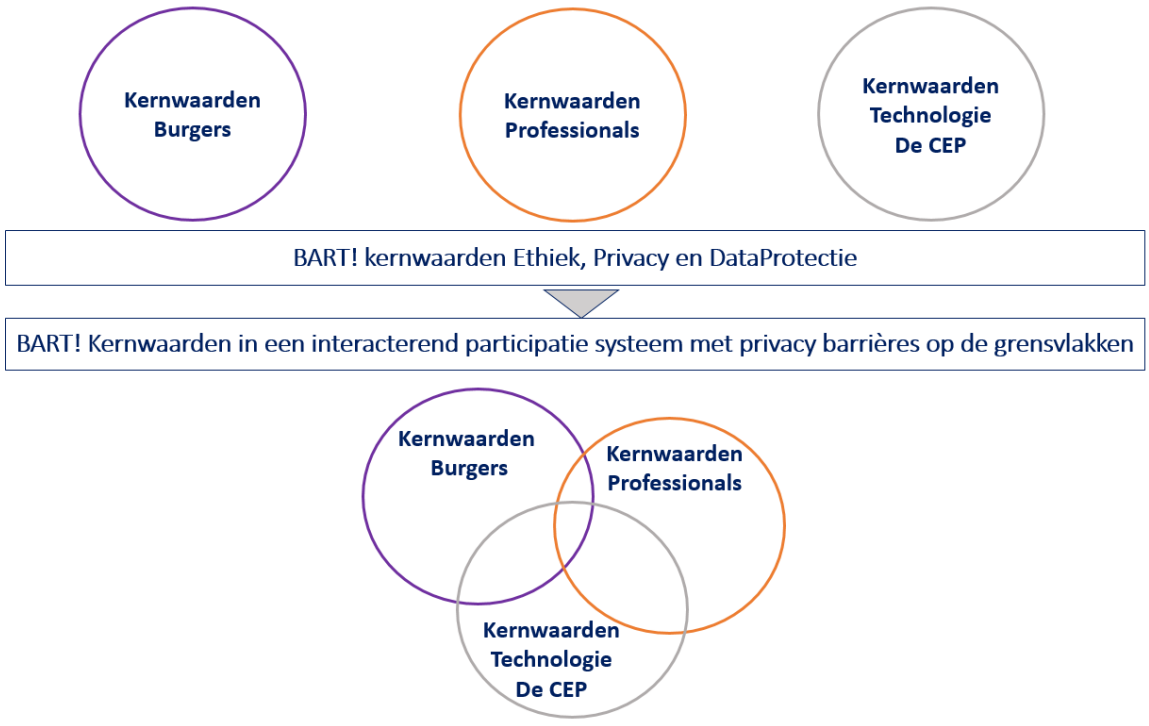
[22] Art. 5, lid 1, sub b AVG en art. 3 Wpg

# 5. Toekomst Ethiek, Privacy en Dataprotectie BART!

Om de in hoofdstuk drie genoemde ethische en wettelijke kaders te betrekken is het noodzakelijk om BART! te splitsen in drie domeinen.

1. Het deelsysteem “burgers” waarin burgers informatie via een digitale buurtgroep met elkaar en met de overheid kunnen delen, waarin de toestemming van burgers voor het gebruik van de door hen aangereikte informatie is geregeld. Burgers moeten hierbij zelf kunnen bepalen met wie zij welke informatie willen delen.
2. Het deelsysteem “Professionals”, waar de gegevens verwerkt worden tot handelingsperspectieven.
3. Het deelsysteem “Technologie“: de intelligente participatietechnologie van BART! (de “Complex Event Processor”), het ondersteunde technische systeem dat op de achtergrond de communicatie tussen burgers en professionals afhandelt.

Deze opdeling vormt dan ook het raamwerk van kaders die gelden voor de functionele en technische specificaties opgesteld vanuit het aandachtsgebied EP&DP.




Dit raamwerk is een eerste aanzet voor het pakket functionele wensen en eisen ten behoeve van de uiteindelijke technische randvoorwaarden en specificaties op basis waarvan BART! aanbesteed zou kunnen worden. De genoemde kernwaarden en toekomstperspectieven komen voort uit een risicoanalyse en het bijbehorende juridische kader.

## 5.1 BART! en de faciliterende technologie

Het deelsysteem Technologie wordt benoemd als faciliterende technologie. De technologie faciliteert de communicatie tussen burgers en overheden. De aanbieder van deze technologie is de verwerkingsverantwoordelijke in de zin van de AVG.

De verantwoording van de overheidsorganisaties[23] brengt onder andere met zich mee dat er beleid moet zijn dat het geheel in overeenstemming is met de AVG respectievelijk de Wpg, met bijbehorende organisatorische en technische maatregelen om de privacy te waarborgen. De verwerker van de gegevens moet op zijn beurt in staat zijn om de regels van de verwerkingsverantwoordelijke te volgen en te implementeren.

Betrokkenen moeten toestemming geven of geïnformeerd worden over de persoonsgegevens die de overheid verwerkt. Op die manier weten betrokkenen dat een partij hun persoonsgegevens wil verwerken. Dit bewustzijn is van belang, omdat de AVG verschillende rechten geeft aan betrokkenen en zonder op de hoogte te zijn kunnen deze rechten niet benut worden.

Informeren kan door toestemming te vragen of door informatie te verschaffen aan betrokkenen indien de verwerking gebaseerd is op een rechtsgeldige grondslag die geen toestemming vereist. Informeren is echter niet altijd nodig, de AVG[24] geeft de uitzondering: informeren is onmogelijk of vergt onevenredige inspanning. In dat geval is er wel een verplichting om naar het publiek in algemene zin te communiceren over de verwerking (hierbij moet informatie over de soort verwerkingen openbaar worden gemaakt).

Als eerste stap kunnen verwerkingsorganisaties algemene informatie openbaar maken waardoor betrokkenen zichzelf kunnen informeren door nieuwsartikelen en websites van de desbetreffende partijen te lezen. Voor de politietaak gelden uitzonderingen op basis van de Wpg[25], waaronder valt dat de politie gemakkelijk van de informatieplicht kan afzien indien het in het belang van een strafrechtelijk onderzoek is.

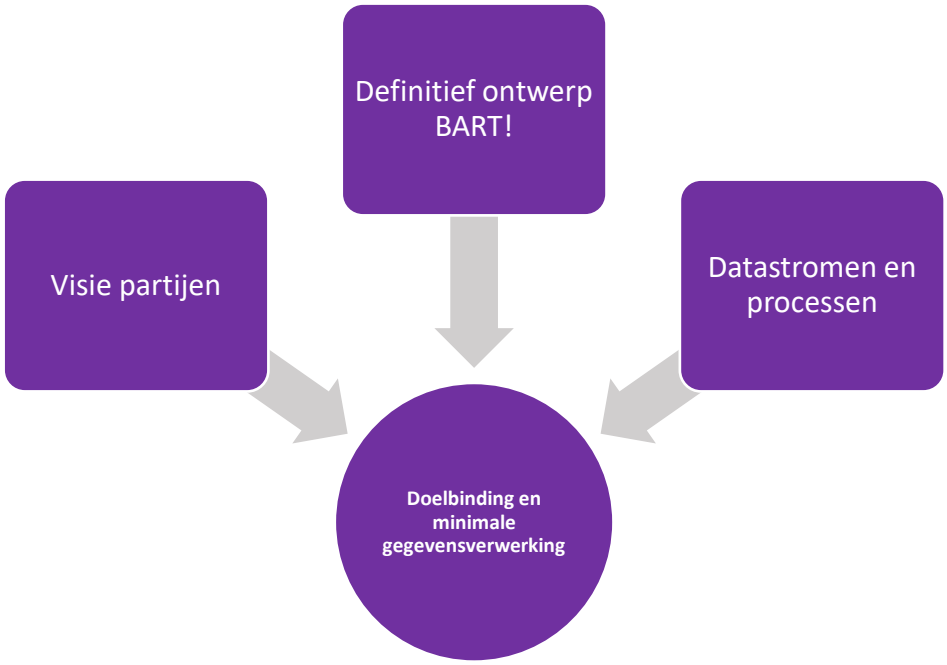
De AVG legt de voorkeur bij individueel communiceren mits dit mogelijk is. Dat wil zeggen dat de betrokkene op de hoogte moet worden gesteld van de verwerking van persoonsgegevens. De overheidsorganisaties die gebruik maken van BART! dragen hier verantwoordelijkheid voor.

De AVG[26] stelt ook vereisten voor doelbinding, hetgeen van belang is voor het proces en de daarop volgende minimale verwerking van persoonsgegevens. Het doel van BART! moet concreet en per partij in kaart worden gebracht, omdat op die manier gekeken kan worden naar de datastromen die wel en niet relevant zijn voor het beoogde doel. Hetgeen niet relevant is mag niet worden meegenomen binnen BART!, omdat BART! daarmee niet aan de voorwaarde van minimale

[23] Art. 24 AVG
[24] Art. 14, lid 5, sub a AVG
[25] Art. 27 Wpg
[26] Art. 5, lid 1, sub b AVG

gegevensverwerking[27] kan voldoen. Die voorwaarde ziet toe op het uitsluitend verzamelen van data die noodzakelijk is. Omwille van de doelbindingen moeten visie, definitief ontwerp en datastromen op elkaar aansluiten, hier mag geen sprake zijn van overbodige processen die onnodige persoonsgegevens verwerken.

De partijen stellen duidelijke doelen in relatie tot de verwachtingen van BART! en de te verzamelen gegevens met bijbehorende output. Dit vergt een definitief ontwerp van BART!, waarbij alle domeinen op een samenhangende manier op elkaar aansluiten. Vervolgens moeten de bijbehorende datastromen en processen worden ingericht om overbodige processen en gegevens uit te sluiten. Naast de benodigde doelbinding zijn de eerdergenoemde proportionaliteit en subsidiariteit belangrijke toetsingscriteria bij het verwerken van persoonsgegevens.




[27] Art. 5, lid 1, sub c AVG

## 5.2 Barrières om het gebruik van persoonsgegevens veilig te stellen

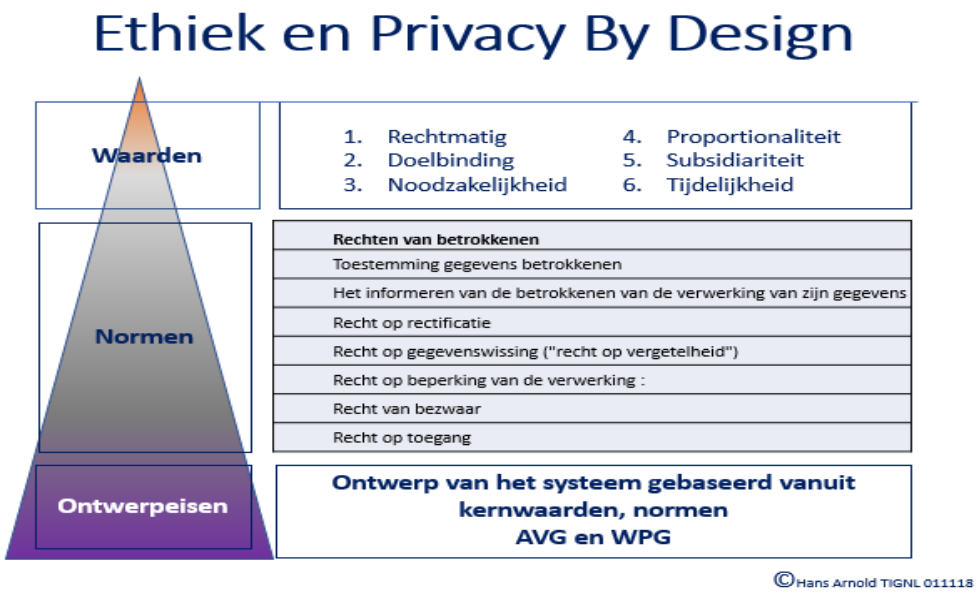
Om overbodige persoonsgegevens uit te sluiten zijn barrières nodig die zowel technisch, sociaal of organisatorisch van aard kunnen zijn. De barrières moeten over het gehele proces worden gepositioneerd om gezamenlijk een barrièremodel te vormen, waarbij alle barrières elkaar ondersteunen. Essentieel zijn barrières aan de voorkant, daar waar de persoonsgegevens worden verzameld.

**BART! barrières**
1) Technische barrières zijn geautomatiseerd en behoeven geen menselijke tussenkomst,
2) Sociale en organisatorische barrières zijn gericht op het menselijk handelen.


In het BART-concept is het wellicht niet mogelijk om alle barrières technisch te implementeren, waardoor de nadruk ook op sociale en organisatorische maatregelen komt te liggen. Dat wil zeggen dat burgers, professionals en overheidsorganisaties verantwoordelijkheden krijgen waarnaar men moet handelen omwille van de gefaciliteerde communicatie door BART!. Technische barrières zijn geautomatiseerd en behoeven geen menselijke tussenkomst, maar sociale en organisatorische barrières zijn juist gericht op het menselijk handelen.

# 6. Kernwaarden, Functionele- en Technische Realisatie

Ethische richtlijnen en privacywetgeving zijn cruciaal voor een fatsoenlijke digitale samenleving. BART! draagt bij aan de kwaliteit van de leefomgeving. Daarom is het essentieel dat ethische en privacy inzichten enerzijds in de architectuur van BART! zijn ingebracht en anderzijds haar ethisch en privacy beleid zijn geborgd in het systeemontwerp.

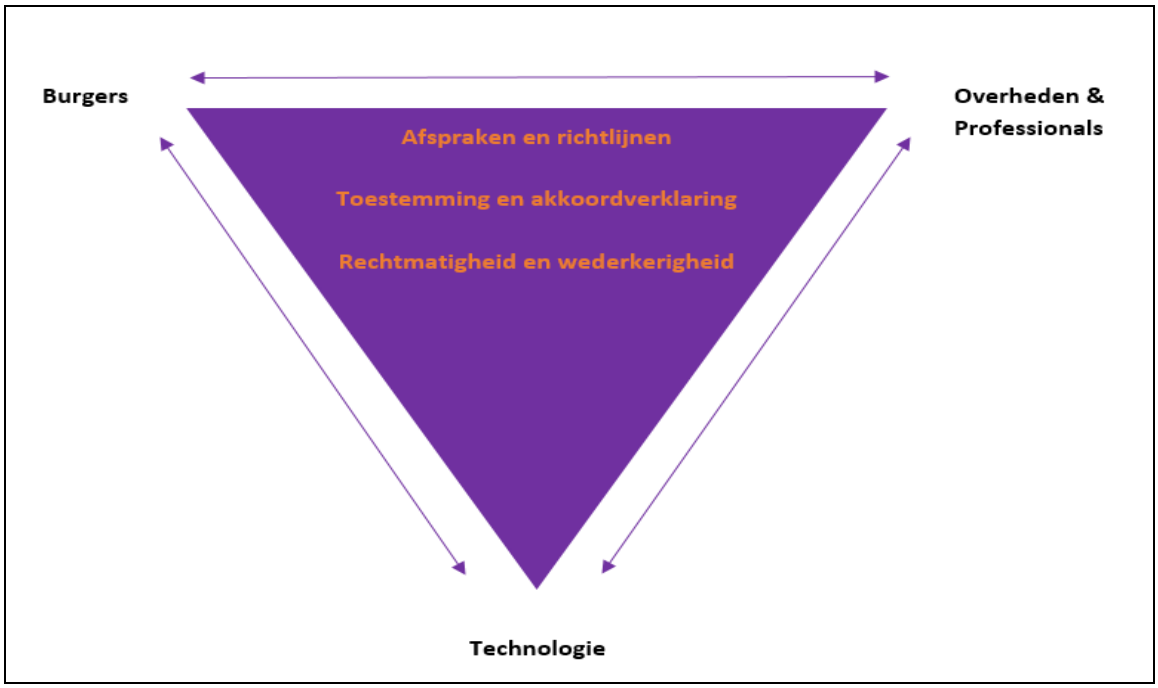



Aansluitend aan kernwaarden zijn normen van toepassing die input geven aan de initiële functionele eisen die op hun beurt weer toekomstperspectieven voor het functionele en technisch ontwerp van BART! bieden.

## 6.1 BART!-driehoek samenwerking en horizontale communicatie

Aan de hand van de toekomstperspectieven kan er een richting worden gekozen of kunnen additionele doelen worden gesteld voor de functionele en technische realisatie. In de opbouw naar de toekomstperspectieven vanuit de kernwaarden, is het essentieel om de interactieve BART!-driehoek te beschrijven, welke bestaat uit burgers, professionals en de technologie.

De BART!-driehoek is een platte driehoek, omdat deze voor participatie staat. Participatie heeft als kenmerk samenwerking en horizontale communicatie tussen de partijen. De technologie is in deze situatie een derde partij die het proces moet verbeteren. In deze context is de technologie een facilitator die op de achtergrond de communicatie tussen burgers en professionals ondersteunt.




Zowel binnen een analoge als binnen een digitale omgeving gelden waarden en normen ten aanzien van ethiek, privacy en dataprotectie. In beginsel liggen de verantwoordelijkheden bij burgers en professionals, die in de participerende sferen afspraken moeten maken. De belangrijkste afspraak tussen burgers en professionals is de afspraak over het verwerken van gegevens op basis van toestemming, hierover volgt meer onder de kop 6.2. Doelbinding is een essentieel onderdeel van deze afspraken, omdat doelbinding aangeeft welke gegevens met welke doel worden verwerkt.

De technologie in de meeste kale en functionele vorm is geen handhaver van waarden en normen. Desalniettemin kan de technologie gedurende het creatieproces wel in die richting gevormd worden. Vanuit deze denkrichting kan technologie uitkomsten bieden om de grip op persoonsgegevens te vergroten. Logischerwijs is technologie niet vanzelfsprekend, waardoor tijdens de creatie goed getest moet worden of alles naar behoren werkt. Technologie mag enkel worden ingezet als de werking is aangetoond.

Waar de kernwaarden vooral aangeven wat de initiële eisen zijn voor de drie domeinen, zal het toekomstperspectief oplossings- en ontwerprichtingen bieden. Zo zijn er mogelijkheden te benoemen die de lasten betreffende verantwoordelijkheden van burgers en professionals verminderen of borgen.

### 6.1.1 De burger als centrale actor

BART! is bedacht om burgers vanuit verschillende overheidsorganisaties beter van dienst te zijn. Essentieel is de input die burgers leveren in de vorm van meldingen. Des te gemakkelijker het is om meldingen te doen, des te meer input kan worden verwacht. In die lijn van redenatie zullen meer aangesloten applicaties zorgen voor een hogere mate van toegankelijkheid. Immers, de burger kan alle applicaties naar voorkeur gebruiken.

De verantwoordelijkheden die de burger krijgt bij het gebruik van BART! zorgen juist weer voor afbreuk van de toegankelijkheid. Burgers kunnen niet willekeurig persoonsgegevens gaan delen en zullen zelf veel verantwoordelijkheid dragen als de ondersteuning vanuit de technologie en de professionals nog niet ver gevorderd is. Tevens heeft privacy invloed op de toegankelijkheid, omdat de burger meer vertrouwen heeft in de overheid als de overheid de privacy op een juiste wijze waarborgt.

Zonder toegankelijkheid kan een participatieproces nooit bestaan, omdat de burger hierin een sleutelrol inneemt. Des te meer verantwoordelijkheden bij de burger liggen, des te groter de drempel om te participeren. Compliance mag nooit enkel berusten op de verantwoordelijkheden van burgers. BART! moet ingericht worden op een manier dat de burger weinig lasten (verantwoordelijkheden) draagt en zo eenvoudig mogelijk rechtmatige meldingen kan maken.

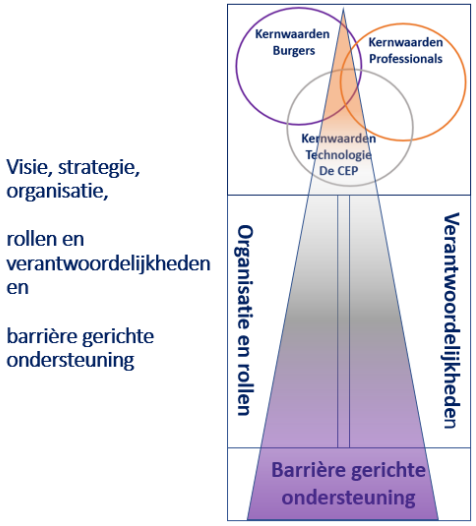
Dit raakt de fundamentele structuur van BART!, welke in beginsel gericht is op het aansluiten van veel verschillende applicaties. In de volgende paragraaf zal dit vraagstuk uitgediept worden.

## 6.2 Verwerkingsgrondslag en barrière gerichte ondersteuning

**BART!** kan verschillende doelstellingen van verschillende overheidsorganisaties faciliteren.

In beginsel is BART! een faciliterende technologie die ervoor zorgt dat de communicatie tussen burgers en overheden volgens participatiewaarden verloopt.

Centraal hierbij staan de verwerkingsgrondslag, de mate van controle en barrières tegen onrechtmatigheden, waar deze paragraaf toelichting over geeft.




### 6.2.1 Verwerkingsgrondslag

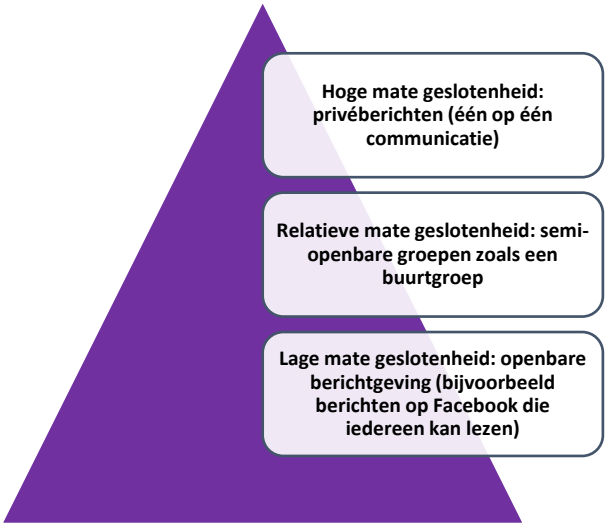
Afhankelijk van de doelbinding van de partijen zijn er rechtmatige verwerkingsgronden waarmee partijen persoonsgegevens mogen verwerken. Hierbij is het belangrijk om op te merken dat de overheidsorganisatie de verwerkingsverantwoordelijke is. Los van de grondslag moet de verwerking altijd proportioneel zijn om niet onevenredig mensenrechten te schenden.[28]

[28] Artikel 8 EVRM. Om de schending van privésferen te toetsen zijn proportionaliteit en subsidiariteit van belang, waar artikel 8 EVRM op wijst.

De grondslag en de doelbinding bepalen of persoonsgegevens uit bepaalde bronnen verwerkt mogen worden. Bij BART! moet hier meer context worden gegeven, omdat de burger zelfs binnen platformen op verschillende manier communiceert. Communicatie kan namelijk openbaar, semiopenbaar (denk aan groepen) of privé zijn. De categorieën zijn: privéberichten (een op een), semiopenbare berichten zoals in groepen en openbare berichten zoals bijvoorbeeld openbare berichten op Twitter of Facebook. Des te meer de communicatie gesloten is, des te minder personen hier deel van uitmaken.

Burgers die toestemming verlenen moeten in staat zijn keuzes te maken over de platformen waarmee zij communiceren. Op die manier kunnen burgers gericht toestemming geven over via welke bronnen gegevens door BART! kunnen worden verwerkt. In de toekomst is het wellicht mogelijk om binnen platformen onderscheid te maken, door per gesprek (bijvoorbeeld een Whatsapp groepsgesprek) of per bericht een opt-in of opt-out mogelijkheid te geven. Toestemming per platform voldoet enkel als de overheid voldoende toelichting geeft over zaken zoals doelbinding.

Dit moet transparant zijn, zodat de burger in staat is de verwerking te overzien om een keuze te maken.




Als burgers keuzes kunnen maken over welke applicaties en berichten BART! mag verwerken, dan kunnen burgers controle krijgen over persoonsgegevens. De voornaamste privacywetgeving [29] heeft namelijk als doel om burgers controle te bieden over hun eigen opgeslagen persoonsgegevens door verschillende rechten in werking te roepen. BART! moet controle over de eigen data dan ook als uitgangspunt nemen, hetgeen ook de vertrouwensrelatie tussen burgers en overheden versterkt. Des te meer controle, des te beter. De beste situatie zou een situatie zijn waarin burgers in zoveel mogelijk detail de keuzes kunnen beheren, bijvoorbeeld door enkel een bepaalde Whatsappgroep of Facebookpagina aan BART! te koppelen.

[29]AVG en bijbehorende richtlijn voor wethandhavingsorganisaties (Richtlijn EU 2016/680)) Richtlijn EU 2016/680 is van toepassing op het strafrecht en is daarom verwerkt in de Wpg en Wjsg, welke van toepassing zijn op de politie en het Openbaar Ministerie. De AVG daarentegen is van toepassing op gemeenten.

Toestemming, controle en keuzes van burgers zijn essentieel voor participatie en voor BART!. Het verzamelen van gegevens is echter ook mogelijk op basis van een andere juridische grondslag. Deze grondslag voldoet alleen niet aan subsidiariteit en proportionaliteit, omdat het doel van BART! participatie is.

Overheden kunnen op basis van het bestaan van een wettelijke grondslag de keuze van de burger ook tenietdoen. In dat geval gaat het om het verwerken van openbare data buiten de toestemming van burgers om. Dit kan enkel op grond van op wetten gebaseerde taken in het kader van het algemeen belang en zolang er wordt voldaan aan proportionaliteit en subsidiariteit. Voor een gemeente is deze grondslag lastig te beargumenteren, maar voor de politie sluit het aan op de taakstelling.[30]

Naast het wel of niet bestaan van deze wettelijke grondslag zijn subsidiariteit en proportionaliteit essentieel. Subsidiariteit geeft aan dat bij de manier van verwerken zo weinig mogelijk sprake moet zijn van inbreuk het privéleven van burgers. Oftewel, als het op een andere manier kan, dan moet deze manier benut worden. Proportionaliteit geeft aan of de zwaarte van de maatregel in balans staat met het doel.

Vanuit het perspectief van subsidiariteit gaat de voorkeur naar een toestemmingsconstructie, omdat participatie anders verschuift naar surveillance. Het doel van BART! is niet om een surveillance-instrument te worden, maar juist een verbindende factor te vormen waarop participatie kan floreren. Een dergelijk surveillance-instrument past ethisch gezien niet bij participatie, omdat participatie niet mogelijk is als overheden de burgers uitsluiten. Daarbij zijn transparantie en betrouwbaarheid fundamenten van ethiek. Aldus, toestemming is belangrijk om de verbondenheid tussen burgers en overheid te concretiseren en om BART! de ethiek te laten borgen.

Het is vanzelfsprekend mogelijk dat overheidspartijen zoals politie en gemeente op bepaalde manieren aan surveillance mogen doen ter bestrijding van ondermijning of ter ondersteuning van handhavingsactiviteiten. Dit vergt echter een aparte toepassing en mag vanwege de zojuist genoemde redenen niet samenvallen binnen BART!.

### 6.2.2 Controle

Vaststellende dat de toestemmingsverklaring die burgers kunnen geven de basis vormt van gegevensverwerking binnen BART!, doet de vraag rijzen wat de stappen zijn om dit te verwezenlijken.

De creatie is vrij van vorm, zolang het maar aansluit op alle relevante applicaties en onder de voorwaarde dat de burger voldoende controle over eigen persoonsgegevens krijgt. Derhalve moeten de instellingen bij aanvang zo privacy-vriendelijk mogelijk ingesteld staan (privacy by default), waarna

[30] Art. 3 en art. 4 Politiewet

de burger keuzes dient te krijgen over via welke platformen (applicaties) en met welke overheden de burger wil participeren. Kortweg vereist dit een apart burgerpaneel en/of aangevulde verklaringen en instellingen in de verschillende applicaties die burgers gebruiken. Zo'n burgerpaneel is vergelijkbaar met de functionaliteit van MijnOverheid, waar burgers een centrale berichtenbox hebben waarbij burgers toestemming geven aan overheden om via die berichtenbox te communiceren.

Hieronder worden in de tabel de toekomstperspectieven ten aanzien van deze kernwaarde toegelicht.

| Vorm | Toelichting |
|---|---|
| **Decentraal - applicaties** | Applicaties kunnen zich -mits zij voldoen aan voorwaarden- bij BART! aansluiten en een BART!-modus implementeren in de instellingen. Burgers kunnen deze modus aanzetten naar wens (privacy by default). |
| **Decentraal met een centraal component - controlepaneel** | In plaats van verschillende instellingen bij verschillende applicaties kan BART! een centraal controlepaneel bieden. In dit paneel kunnen burgers overheden selecteren waarmee zij willen participeren. Tevens kan de burger een selectie maken uit aangesloten applicaties. Deze instellingen worden vervolgens automatisch doorgezet naar de applicaties die de burger aangevinkt heeft. Hierdoor ontstaat standaardisatie van BART!-instellingen. |
| **Centraal - een BART!-applicatie** | Een BART!-applicatie kan nog meer controle bieden aan de burger. Daarnaast kan het de burger ondersteunen met het op een legitieme wijze delen van persoonsgegevens. Aldus, een BART!-applicatie kan meer grip bieden op het naleven van de waarden en normen door daar waar persoonsgegevens worden verzameld invloed uit te oefenen. Denk hierbij aan een stappenproces per melding met uitleg en tools (filters om persoonsgegevens te blurren) om de input doelmatig en minimaal te houden. Een centrale applicatie kan op die manier een barrière vormen aan de voorkant van het proces, direct bij de input. |
| **Combinatie** | Combinaties zijn mogelijk om maatwerk te leveren aan de burger. De burger is in essentie variabel. De ene burger wenst meer controle/ondersteuning dan de ander. Niet onbelangrijk zijn privacy- en veiligheidsrisico's bij het gebruik van diensten van derde partijen (zie 6.2.3).<br><br>Het is denkbaar om verschillende applicaties aan te sluiten voor de communicatie van overheid richting burger. Denk hierbij aan een waarschuwingsmelding over afval midden op straat. Zodoende kunnen burgers 'niet privacygevoelige' informatie ontvangen op applicaties naar keuze. Zodra burgers meldingen willen doen gaat de voorkeur uit naar een centrale applicatie met afgeschermde een op een communicatie. |

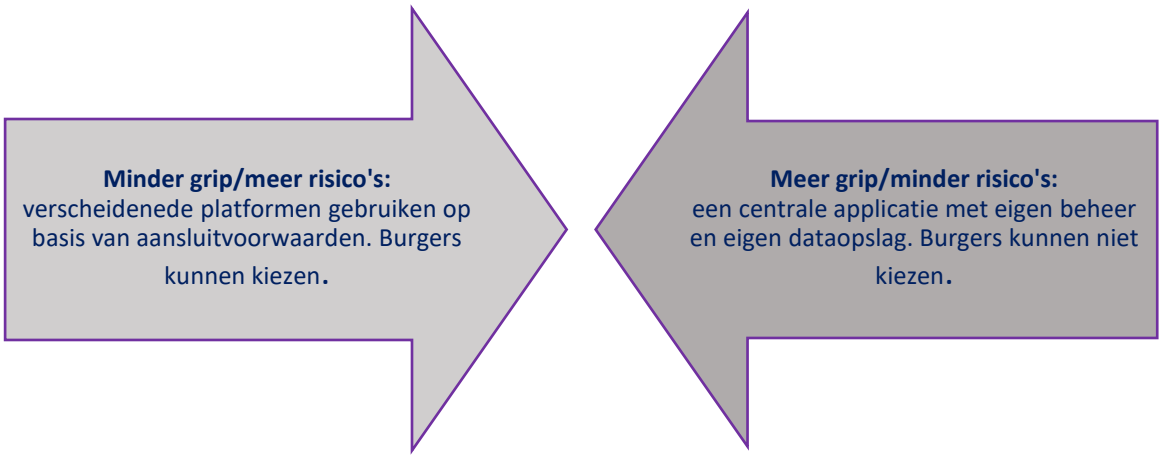
### 6.2.3 Platformen, gegevensuitwisseling, opslag en derde partijen

In de bovenstaande tabel zijn verschillende mogelijkheden toegelicht die gericht zijn op de gegevensstromen van de burger richting de overheid en andersom. Omdat BART! maatwerk wil leveren aan de burger en in hoge mate toegankelijk wil zijn, loopt de communicatie tussen burgers en professionals via verschillende applicaties van derden.

Het is uiterst belangrijk om vast te stellen dat communicatie tussen burgers en professionals ook binnen de opslag van deze derde partijen valt. Denk hierbij aan de servers van diverse social mediabedrijven. Dergelijke bedrijven slaan de data op, om de diensten die zij aanbieden in stand te houden. Immers, anders zouden burgers geen berichten van elkaar kunnen lezen. Ondanks dat deze partijen gebonden zijn aan de AVG zijn er risico's.

Het voornaamste risico is dataopslag in het buitenland, buiten de controle van de overheidsorganisaties waar de burger mee communiceert. Privacy hangt in dat geval af van de maatregelen van de derde partijen, waardoor overheidsorganisaties en burgers grip verliezen. De data moet worden opgeslagen binnen Nederland of in ieder geval binnen de EU om privacywetgeving te handhaven en niet afhankelijk te zijn van andere landen.

Een maatregel die derde partijen kunnen nemen is de end-to-end encryptie, beveiliging waardoor berichten enkel door de gesprekspartners kunnen worden gelezen. Het gebruik hiervan dekt de vertrouwelijkheid van de communicatie, door data ontoegankelijk te maken voor de aanbieder van de dienst.  Buiten dergelijke maatregelen om is het alsnog van belang dat burgers en professionals zo weinig mogelijk persoonsgegevens en andere gevoelige informatie versturen via platformen die in handen zijn van derde partijen. Voor het gebruik van platformen voor BART!-communicatie moeten strenge voorwaarden worden gesteld die ervoor zorgen dat burgers en overheden voldoende grip hebben op de data. Ook kan overwogen worden om een centrale applicatie te gebruiken onder eigen beheer. De strenge voorwaarden moeten worden getoetst door middel van een risicoanalyse over persoonsgegevens.



Bij beide richtingen is toegankelijkheid een belangrijk onderwerp. Het is noodzakelijk om strenge aansluitingsvoorwaarden te stellen, zodat burgers kunnen kiezen uit veilige opties. De keuze van de burger is afhankelijk van de uitkomsten van de risicoanalyses betreffende aansluitingsvoorwaarden in meer of mindere mate beperkt. Bij het centraliseren door middel van een eigen applicatie met eigen beheer is de keuze volledig uitgesloten in ruil voor grip op dataopslag en input.

De professional is voornamelijk aanwezig bij de achterkant van het gegevensverwerkingsproces zoals in de volgende paragraaf aan bod komt. Daarentegen vormen burgers de voorkant van het proces door input te leveren in de vorm van meldingen. Burgers mogen bij het maken van meldingen niet zomaar persoonsgegevens van anderen delen als dit niet proportioneel is. De overheid moet via de professionals de burger ondersteunen door verantwoordelijkheid te nemen voor het zorgdragen van de rechtmatige gegevensverwerking.

Beide partijen moeten voorzichtig zijn met de gegevens die zij delen via platformen in handen van derden. Zoals gesteld in de kernwaarden dragen zowel burgers als professionals verantwoordelijkheid. Technologie kan deze verantwoordelijkheden verlichten door ondersteuning (of volledige automatisering) te bieden.

## 6.3 Verantwoordelijkheden – voor- en achterkant

Burgers en professionals hebben verantwoordelijkheden als het gaat om het delen van persoonsgegevens. Burgers en professionals moeten rekening houden met verschillende zaken. In beginsel landen deze zaken op een analoge (zonder tussenkomst van technologie) wijze bij burgers en professionals. Dat wil zeggen, dat de barrières voor onrechtmatigheden rondom privacy, ethiek en dataprotectie berusten op de mate van bewustzijn, kennis en bijbehorende handelingen van burgers en professionals.

### 6.3.1 Verantwoordelijkheden burgers

Zoals is af te leiden uit de kernwaarden vallen de lasten om aan de waarden en normen te voldoen op de participerende burger en de professionals. Omdat de overheidsorganisaties de participatie aanjagen dragen zij een verantwoordelijkheid die zich uit in de zorgtaak van de professional. Zo moet de professional zorgdragen dat er afspraken gemaakt en nageleefd worden met en door de burger. Mocht de burger hierin tekortschieten, dan is de professional de poortwachter die onrechtmatigheden kan voorkomen. Dit stelt eisen aan de verwerkingsverantwoordelijke organisaties, omdat zij de professionals die daar werkzaam zijn moeten ondersteunen met beleid en andere handvatten over ethiek, privacy en dataprotectie.

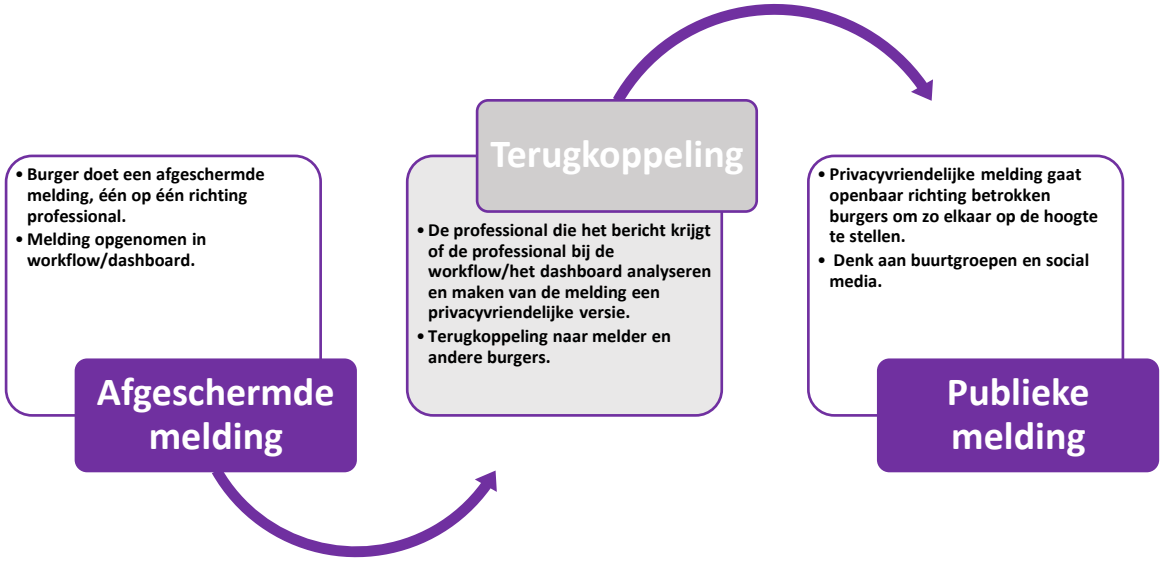
De burger die wil participeren moet in beginsel op een aantal zaken letten zoals het versturen van meldingen met persoonsgegevens. Deze gegevens mag de burger niet altijd vastleggen vanwege proportionaliteit. Echter, burgers zijn geen onderdeel van een organisatie die toeziet op deze afwegingen, waardoor de burger afhankelijk is van eigen inzicht en ondersteuning van professionals.

Belangrijk is dat burgers meldingen niet openbaar doen, maar via een afgesloten communicatiegang naar een professional of organisatie. Dit kunnen privéberichten zijn naar een wijkagent of een anderszins afgeschermd bericht gericht aan een overheidsorganisatie. Dit is van belang, omdat burgers niet zomaar persoonsgegevens van anderen mogen openbaren.

De meest pakkende voorbeelden die hierbij gegeven kunnen worden zijn schoolfoto's of andere groepsfoto's die burgers dagelijks delen op social media. Stel dat het niet gaat om een groepsfoto na een middag voetballen, maar om een foto van een geweldsincident (vechtpartij). Deze beelden kunnen onevenredig de personen in kwestie schaden, doordat zij herleidbaar in beeld zijn gebracht binnen een negatieve context. Om deze redenen mag de burger enkel openbare meldingen doen als deze geen herleidbare persoonsgegevens bevatten. Dit sluit aan op de verantwoordelijkheid van de overheid om zorg te dragen voor de rechtmatige verwerking van persoonsgegevens.

Het melden van de kleur van de jas, de grote van een groep of andere globale kenmerken is wel toegestaan. Dit klinkt allemaal heel logisch, echter ligt de uitvoering bij de burger. Eerder is aangegeven dat professionals hierin een zorgtaak hebben.

Het is noodzakelijk om de communicatie tussen burgers en professionals vast te leggen in eenvoudig te volgen processen. Een eerste stap is om de communicatie (melding) via afgeschermde kanalen te voeren, tussen melder en professional. Hierna kunnen melder en professional gezamenlijk de melding bewerken (indien nodig) om het vervolgens te communiceren richting andere burgers. Op deze wijze begaan burgers geen schendingen van privacy en kan de professional zijn of haar taak als ondersteuner en poortwachter beter uitvoeren.




Het bovenstaande proces berust in dit schema op de acties van professionals. Technologie kan deze acties ondersteunen door geheel of deels geautomatiseerd persoonsgegevens en haatzaaiende termen te herkennen. Hierover volgt meer in paragraaf 6.7 over de ontwikkeling van technologie binnen de kaders van BART!.

### 6.3.2 Professionals als zorgdragers en poortwachters

De professional is binnen het BART!-proces de poortwachter die onrechtmatigheden buitensluit en gewenste zaken doorlaat. Noemenswaardig is dat de poortwachter positie inneemt achter het verwerkingsproces. De professional krijgt de informatie door uit de verwerkingsunit (technologie) en dan pas kan de professional handelingen verrichten. Ondanks dat de professional de burgers kan beïnvloeden en bewustmaken blijft er afstand bestaan. Immers, de professional zit niet naast de burger wanneer de meldingen worden gemaakt.

In de vorige paragraaf is beschreven dat de professional de burgers moet aansturen om in eerste instantie enkel een op een te communiceren. Dit sluit communicatie tussen burgers onderling niet uit, maar bewaakt wel het verspreiden van persoonsgegevens. Burgers onderling kunnen op basis van de terugkoppeling waarin gevoelige gegevens zijn weggelaten met elkaar interacteren. Burgers kunnen volop interactie aangaan zonder dat iedereen de belastende persoonsgegevens kan inzien. Een terugkoppeling in real time is hierbij erg belangrijk. Burgers kunnen aan de hand van de terugkoppeling in real time de privacy-vriendelijke versie van de melding direct ontvangen. Door de hoge snelheid van de terugkoppeling blijft de kans op interactie ontstaan. Zo kunnen burgers met elkaar in gesprek om elkaar te wijzen op zaken zoals openstaande ramen of een omgevallen afvalcontainer. Een wijkagent of een community-builder kan hier ook een rol in spelen door de interactie aan te jagen of door mee te doen aan het communicatieproces tussen burgers.

Vanuit het privacy-perspectief is de professional een belangrijk element, maar op zichzelf staande niet voldoende. De verantwoordelijkheden zijn niet alleen voor de professional, maar ook voor de organisatie (verwerkingsverantwoordelijke). Zaken als de rechten van betrokkenen en de informatieplicht zijn in beginsel allemaal gerelateerd aan de reguliere opslag binnen de organisatie. Bij het BART!-ontwerp is het niet verstandig om direct alle data bij de reguliere opslag van de diverse organisaties te voegen. Omdat de professional de poortwachtersfunctie moet vervullen zal er ook een poort in de vorm van een aparte opslagruimte aanwezig moeten zijn. Eerder is aangegeven dat de technische verwerkingsunit de data in real time moet verwerken, zodat gegevens niet worden opgeslagen (kernwaarde 2 – Technologie, zie 4.3). Vervolgens worden de gegevens doorgestuurd naar het dashboard (of andere vorm) waar vervolgacties binnen de organisatie plaatsvinden. Hierbij is de vraag hoe de datastromen moeten lopen.

Bij de vormgeving van datastromen is de centrale vraag of de gegevens die gepresenteerd worden in het dashboard ook in een aparte database binnen de organisatie dienen te worden opgeslagen. Een aparte database kan de organisatie meer controle bieden door ook hier technische en organisatorische maatregelen (privacy by design) te treffen zoals korte bewaartermijnen, aangepaste autorisatie en afgeschermde toegang. In eerste instantie valt dit buiten de scope van BART!, maar het is wel essentieel voor de werking en de rechtmatigheid van het gehele proces. De aparte database die zojuist is toegelicht is als het ware een sluis, een tussenstation van data.

In het kader van het sluisontwerp kunnen de volgende gradaties worden aangebracht. De meldingen komen binnen op het dashboard en worden opgeslagen in een opslag gekoppeld aan het dashboard. Zoals te zien op de bovenstaande afbeeldingen vormt het paarse vlak een sluis in het proces tussen de verwerking en het doorzetten van de data naar reguliere databases binnen de organisatie.

De opslag is in dit geval gericht op zeer korte termijnen, waarbij de professional meldingen analyseert, afhandelt, vernietigd of doorzet. Zodra de meldingen worden doorgezet komen de gegevens terecht in een andere database van waaruit de organisaties zorg moeten dragen voor de rechten van betrokkenen en de informatieplicht.

Opgemaakt kan worden dat snelheid een belangrijke factor is bij de inrichting van het proces en dat afscherming van gegevens in verschillende fases verplicht is. Immers, een hoge snelheid bij het analyseren van gegevens heeft effect op minimale gegevensverwerking. Als gegevens snel worden vernietigd, dan blijft de hoeveelheid opgeslagen gegevens beperkt. Door gegevens snel te behandelen, te vernietigen of door te zetten ontstaat een hoge datamobiliteit (verkeersstroom), waardoor niet onrechtmatig veel gegevens (minimale gegevensverwerking) worden opgeslagen.


Een aparte dataopslag voor BART!-data is noodzakelijk, maar niet voldoende. Om te voorkomen dat meldingen niet zomaar worden doorgezet, is het van belang dat er aansluitende organisatorische maatregelen worden genomen. Denk hierbij aan logging, autorisatieprofielen en een verificatieproces.

Daarnaast kan het zinvol zijn om de zeer korte bewaartermijn modulair te installeren. Dat wil zeggen dat niet iedere binnenkomende melding dezelfde bewaartermijn krijgt van bijvoorbeeld 24 tot 48 uur. Sommige meldingen zijn ‘zwaarder’ dan andere meldingen, denk hierbij aan het verschil tussen afval op straat tegenover een uit de hand gelopen demonstratie (openbare orde in geding).

Tijdelijkheid is een fundament in de privacywetgeving. Vandaar dat een aparte database van belang is, waarin in alle meldingen terechtkomen. Zodoende is het aan te bevelen om gradaties mogelijk te maken die door de professional achter het dashboard of met toegang tot de workflow kan worden ingesteld. Bijvoorbeeld: een lage categorie met een korte bewaartermijn, bijvoorbeeld 24 uur; een middelzware categorie met een middellange bewaartermijn, bijvoorbeeld 48 uur en een zware categorie met een lange daarop van toepassing zijn bewaartermijn, bijvoorbeeld 72 uur. In dat geval kan er een balans gevonden worden tussen het waarborgen van de privacy en de praktijk die professionals ervaren. Meldingen die echt noodzakelijk zijn en een ‘staartje’ krijgen kunnen op deze manier binnen een praktisch tijdbestek worden doorgevoerd, terwijl afgehandelde meldingen en meldingen zonder noodzaak van een snelle vernietiging genieten die de privacy van burgers

waarborgt. Afhankelijk van de organisatie, de capaciteit en de ondersteunende technologie kunnen de bewaartermijnen in uren, dagen of eventueel weken worden ingesteld.

## 6.4 Input, verwerking en output

Zoals eerder besproken geven burgers toestemming voor de wijze waarop hun persoonsgegevens verwerkt mogen worden onder bepaalde voorwaarden. In deze participatiesfeer lenen burgers oren en ogen aan overheden om gezamenlijk de kwaliteit en veiligheid van de leefomgeving te waarborgen. Dit gaat gepaard met het delen van data over bepaalde situaties zoals afval op straat of het signaleren van een inbreker. De verschillende situaties waarmee de burger te maken krijgen kunnen ook wel de variabele context worden genoemd.

Wat soortgelijke situaties met elkaar gemeen hebben is dat het gaat om zaken en persoonsgegevens van anderen dan de melder. De verzamelde persoonsgegevens zullen daarom niet enkel betrekking hebben op de melder (met verleende toestemming), maar juist op personen binnen de variabele context. Vooral als het gaat om beelden (foto's en video's) kunnen er ook persoonsgegevens op de achtergrond in beeld zijn (kentekens, gezichten etc.). Het verwerken van dit soort gegevens kan enkel als de verwerking proportioneel, doelmatig en minimaal (doelbinding en minimale gegevensverwerking[31]) is. Welke persoonsgegevens verwerkt mogen worden hangt daarmee af van de situatie en de bijbehorende proportionaliteit.

Omdat iedere situatie anders is, dragen burgers en professionals veel verantwoordelijkheid om de rechtmatigheid van de verwerking juist in te schatten. De burger heeft verantwoordelijkheden die geïnterpreteerd kunnen worden als lasten. Vanuit dat perspectief vormen de verantwoordelijkheden een obstakel voor de participatie, omdat het afbreuk doet aan toegankelijkheid. Daarnaast heeft de professional in de wijk of achter het meldingendashboard de taak de burger hierin te ondersteunen terwijl de professional ook de poortwachter is voor een rechtmatige verwerking richting de organisatie.

## 6.5 Technische maatregelen in het ontwerp

Zowel de AVG als de Wpg hebben privacy door middel van ontwerp (privacy by design), privacy door middel van standaardinstellingen (privacy by default) en beveiliging van persoonsgegevens hoog in het vaandel staan.[32] Al deze vormen van maatregelen moeten ervoor zorgen dat de basisbepalingen zoals doelbinding, tijdelijkheid, juistheid en minimale gegevensverwerking worden nageleefd.

Privacy door middel van standaardinstellingen is eerder behandeld in paragraaf 6.2. Privacy en beveiliging (dataprotectie) in het ontwerp zijn essentieel, omdat zowel de AVG als de Wpg

[31] Art. 5 AVG
[32] Art. 25 en 32 AVG en Art. 4a en 4b Wpg

meermaals hameren op organisatorische en technische maatregelen. Organisatorische maatregelen zijn zaken als processen en autorisaties die reeds bestaan binnen de organisatie. Technische maatregelen daarentegen zullen als barrières in de technologie moeten worden geïmplementeerd. Door voldoende technische maatregelen te treffen kan de verwerkingstechnologie privacy en dataprotectie waarborgen.

Ten eerste zijn pseudonimisering en versleuteling (encryptie) van persoonsgegevens twee primaire technische maatregelen. Dat wil zeggen dat persoonsgegevens het individu niet herleidbaar maken, zonder dat er andere aanvullende gegevens worden gebruikt. Dit gaat samen met versleuteling, waarmee data zoals persoonsgegevens ontoegankelijk (onleesbaar) kunnen worden gemaakt, behalve voor professionals die geautoriseerd zijn om de data te open met een datasleutel. Door deze maatregelen zijn persoonsgegevens niet in een oogopslag geheel zichtbaar en te koppelen aan een individu.

Ten tweede, het verwerkingssysteem dient beveiligd te worden op basis van risicomanagement. Dat wil zeggen dat er beveiligingsmaatregelen genomen moeten worden op basis van de beveiligingsrisico's zoals de gevoeligheid van de data, de mate waarin deze beschikbaar moet zijn en de hoeveelheid data. Op deze manier kunnen de vertrouwelijkheid, integriteit, beschikbaarheid en robuustheid gegarandeerd worden. Met andere woorden, het systeem werkt goed (vertrouwelijk) en is juist afgeschermd om praktijken zoals datalekken te voorkomen.

Tot slot, er moeten technische maatregelen genomen worden om BART! en de aangesloten systemen bij overheidsorganisaties beschikbaar te houden in tijden van nood. Denk hierbij aan stroomuitval of een ander soort fysiek of technisch incident die het systeem raakt. Tijdig herstel is noodzakelijk om toegang te krijgen tot persoonsgegevens. Dit is ook essentieel om te voldoen aan de rechten van betrokkenen. Als het systeem is uitgevallen, dan is de data niet bereikbaar. En in dat geval kan de overheid niet voldoen aan rechten van betrokkenen zoals de rectificatie of vernietiging van persoonsgegevens. Het geheel van deze technische maatregelen moeten getest en beoordeeld worden op effectiviteit. Denk hierbij aan penetratietesten van de systemen, om te achterhalen hoe kwetsbaar het systeem is en of er persoonsgegevens in gevaar komen.

## 6.6 Rechtmatige verwerking via barrières

Om tot een rechtmatige verwerking te komen moeten barrières opgeworpen worden om onrechtmatige gegevensverwerking te voorkomen. Deze barrières zijn ook de maatregelen die burgers en professionals ondersteunen of zelfs een proces volledig overnemen (automatiseren).

Omdat een enkele barrière niet voldoende is, is het aan te raden meerdere barrières op te werpen die elkaar ondersteunen. Hieronder volgt een tabel met barrières per domein, waarin mogelijkheden (het toekomstsperspectief) worden uitgezet. In de onderstaande tabel staan mogelijkheden kort benoemd die gedurende dit stuk zijn besproken of nog worden besproken.

| Domein/ mogelijkheden | Burgers (voorkant) | Technologie (verwerking) | Professional (achterkant) |
|---|---|---|---|
| Analoge basis | De burger heeft voldoende kennis, inzicht en verantwoordingsgevoel, waardoor de burger bewust de juiste persoonsgegevens deelt. | Het betreft een analoge basis, waarop de technologie slechts de meldingen doorvoert naar de juiste partij. Aldus, geen technische maatregelen ten behoeve van ethiek, privacy en dataprotectie binnen de verwerkingsunit. | De professional is in staat alle onrechtmatige gegevens te verwijderen. Daarnaast moet er een aparte opslag zijn (een sluis) om te voorkomen dat onrechtmatige gegevens binnen de organisatie worden opgeslagen. |
| Tekortkomingen, relativering en mogelijkheden | Menselijk falen is reëel, zeker op basis van snelle handelingen met eventueel emotionele invloeden. Persoonlijke en toegankelijke ondersteuning is nodig. Overheden moeten zorgdragen voor een rechtmatig participatieproces. | De technologie ondersteunt de partijen niet. De technologie moet gaan signaleren en eventueel zelfs geautomatiseerd handelen. Daarnaast moeten voldoende technische ontwerpmaatregelen geïmplementeerd worden zoals versleuteling, pseudonimisering en een adequate beveiliging. | Ondersteuning in de vorm van beleid is nodig. Daarnaast zijn technische waarborgen nodig om doorvoer en opslag van gegevens naar en binnen de organisaties te voorkomen. |
| Ontwikkelingsmogelijkheden technologie en ontwerp | Een BART!-applicatie waarin de burger ondersteuning krijgt en door middel van een stappenplan en bijbehorende tools (zie de tabel onder de kop Verwerkingsgrondslag & Controle). En/of één op één communicatie bij aanvang en creatie melding met ondersteuning van professionals. | Deels of geheel regulerende technologie (zie volgende figuur). Dit is specifiek van toepassing op de verwerkingsunit in tegenstelling tot andere technologische maatregelen. De BART!-applicatie en de ontwerpkaders betreffende opslag ven verwijdering van gegevens bij professionals zijn additionele maatregelen.<br>Voldoende ontwerp maatregelen om privacy en dataprotectie te borgen. | Automatisch meldingen verwijderen binnen zeer korte termijn. De meldingen komen in een aparte digitale ‘selectiebak’ (de sluis) die enkel toegankelijk is voor professionals (logging/autorisatie). Het automatisch verwijderen functioneert als extra waarborg indien de professional tekortschiet. De afgeschermde dataopslag beperkt het effect van onrechtmatigheden. |

Uit de tabel blijkt dat er in meer of mindere mate technologische ondersteuning, regulering en ontwerpkaders nodig zijn om te voldoen aan ethiek, privacy en dataprotectie.

Omdat er verschillende mogelijkheden zijn, zijn er verschillende afwegingen te maken die resulteren in een combinatie van barrières tegen onrechtmatigheden (maatregelen). Centraal staat dat de technische maatregelen in het ontwerp essentieel zijn, evenals de mogelijkheden om de technologie verder te ontwikkelen om de verantwoordelijkheden van burgers en professionals af te vangen en de processen van beide partijen te ondersteunen of geheel over te nemen (automatiseren).

## 6.7 Ontwikkeling technologie – verwerking

Om beide partijen, de burgers en de professionals, te ondersteunen en de rechtmatigheid te waarborgen zijn maatregelen nodig in de technologie. Deze maatregelen variëren van minimumeisen tot aan een volledig geautomatiseerd toekomstbeeld dat niet enkel gericht is op ondersteuning, maar juist (bijna) alle handelingen bij burgers en professionals weghaalt.

### 6.7.1 Ondersteunende en regulerende technologie

Omwille van afbakening is het belangrijk om te melden dat de grens van de mate van regulerende technologie ligt bij het geven van informatie aan de professionals bij overheidsorganisaties. Het daadwerkelijk voorschrijven van handelingen valt onder geautomatiseerde besluitvorming en dat terrein ligt voor nu buiten de scope van BART!. In deze paragraaf volgt een stroomschema waarbij de ontwikkeling van de technologie en de verwerking van persoonsgegevens centraal staat. Het schema bevat geen complete lijst met eisen aan de technologie, maar tracht slechts de verschillen tussen gradaties van ontwikkeling aan te geven. De vereisten voor de technologie komen hierna aan bod.

Kortweg is het BART!-proces waarbij de technologie enkel als doorvoermechanisme functioneert volledig afhankelijk van de sociale- en organisatorische factoren (burgers en professionals) om te voldoen aan de gestelde waarden en normen. Het doorvoermechanisme kan werken als daar omheen voldoende technische, sociale en organisatorische maatregelen worden getroffen zoals de Europese en nationale privacy gerelateerde wet- en regelgeving (AVG en Wpg) voorschrijven. Dit betreft maatregelen buiten de verwerkingstechnologie die van toepassing zijn op de voor- en achterkant.

Een verzameling van maatregelen die zijn geïmplementeerd in de technologie kunnen we duiden als ondersteunende technologie. Ondersteunende technologie kan op een passieve en reactieve wijze zorgdragen voor het waarborgen van ethiek, privacy en dataprotectie. Dit kan door persoonsgegevens of andere zaken waar te nemen via herkenning en vervolgens een melding aan de professional te maken en eventueel de meldende burger.

Er kan gesproken worden over regulerende technologie zodra de technologie op basis van de geïmplementeerde maatregelen zelfstandig gaat acteren. In dat geval vervult de regulerende technologie een proactieve rol door handelingen uit te voeren om de gegevens die zijn onttrokken uit de bronnen, rechtmatig door te zetten en te communiceren met burgers en professionals over de melding. Het handelingsperspectief van de technologie is in die situatie geavanceerder, doordat het mogelijk is om naast waarnemen en melden ook zelfstandig en met maatwerk te acteren. Denk

hierbij aan het weren van meldingen of het eventueel bewerken van meldingen die een onevenredige hoeveelheid persoonsgegevens bevatten in vergelijking met het aan de melding gekoppelde label. Dit is volledig gebaseerd op proportionaliteit, waarbij voornamelijk persoonsgegevens bij meldingen met een lage impact worden beschermd. Daarbij kan deze functie ook deels worden toegepast, door bijvoorbeeld relatief zwaardere meldingen over te laten aan de professionals en te ontsluiten van
technische ingrepen.

Regulerend staat dan ook synoniem voor acterende technologie. Een vervolgstap is aan de acterende technologie mandaat toe te voegen, zodat geautomatiseerde besluitvorming plaats kan vinden. Dit vergt wel een verder ontwikkelde AI-component, omdat AI-basistaken van de analisten gaat overnemen. Het op AI gebaseerde systeem zal dan doorontwikkeld moeten worden om meer gegevens te herkennen, acties uit te voeren en bijbehorende handelingsperspectieven uit te zetten.


Vanuit het toekomstperspectief is regulerende technologie (en geautomatiseerde besluitvorming al helemaal) een vergezicht en aanvankelijk zullen de technische maatregelen rondom ethiek, privacy en dataprotectie in beginsel gericht zijn op ondersteuning. Naar mate er meer technische maatregelen genomen worden die professionals en burgers ondersteunen ontstaat er een beweging naar regulerende technologie. In dat geval zal de technologie steeds meer een regulerende technologie worden. Hierin kunnen organisatorische voorkeuren worden meegenomen, omdat het wellicht wel of juist niet wenselijk is om de lijn van ondersteuning naar regulatie door te trekken.

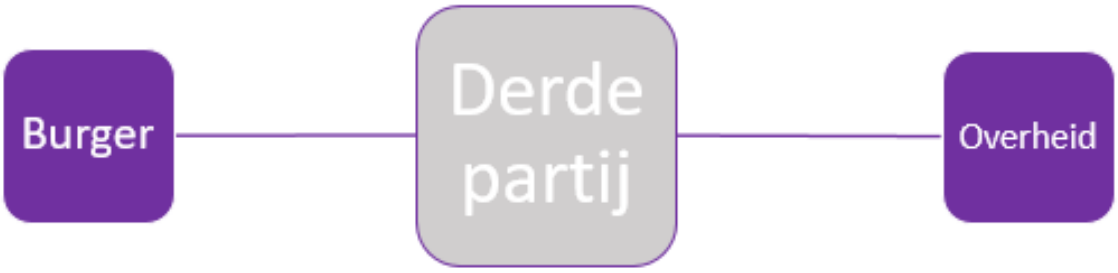
Bij ondersteunende en regulerende technologie is een verbinding vereist tussen de labelingstechniek en de proportionliteitsmatrix van overheidsorganisaties gebaseerd op de gestelde doelen. Het moet namelijk mogelijk zijn om ieder label te koppelen aan een bepaalde mate van proportionaliteit.
De labelingstechniek is het deel van de verwerkingsunit dat meldingen koppelt aan de juiste organisatie met behulp van labels die onderwerpen aanduiden zoals overlast, diefstal en zwerfafval.

Een proportionaliteitsmatrix[33] is een overzicht waarin per label staat welke persoonsgegevens toegestaan zijn per organisatie. Aan de hand van de matrix kunnen professionals de juiste afwegingen maken om persoonsgegevens te weren of juist op te slaan. Binnen de technologie moet dit kenbaar zijn, omdat de verschillende labels gekoppeld aan proportionaliteit invloed hebben op rechtmatigheid. Bij afval op straat mogen niet alle kentekens van alle geparkeerde auto's inclusief beelden van voorbijlopende hondeneigenaren doorgezet worden. De technologie kan dit herkennen mits de labelingstechniek en de proportionaliteitsmatrix juist geformuleerd en geïmplementeerd worden.

### 6.7.2 Verdieping regulerende technologie

Met betrekking tot regulerende technologie is het belangrijk om te begrijpen dat de essentie ligt op het creëren van een (autonome) technologische partij die opereert tussen alle partijen. Dat wil zeggen dat de technologie een controlefunctie heeft en de gemaakte afspraken handhaaft. Bij BART! zijn dat de gemaakte afspraken over ethiek, privacy en dataprotectie gebaseerd op gedeelde waarden en normen. Autonomie heeft in dit geval betrekking op de mate waarin de technologie alleenstaand kan handelen zonder primaire of ondersteunende handelingen van de mens.

De term regulerende technologie is vaak van toepassing op netwerken met een vertrouwensprobleem die een derde partij willen vermijden. Immers, de derde partij die de regulerende functie op zich neemt, neemt een machtspositie in. Technologie kan hier een uitkomst bieden door wet- en regelgeving om te zetten in code, om vervolgens de technologie deze code uit te laten voeren. Het streven daarbij is naar 'law is code', een situatie waarin wet- en regelgeving is omgezet in code en de bijbehorende technologie door middel van code de wet- en regelgeving kan naleven. In dat geval is compliance niet meer afhankelijk van de mens, maar van de technologie, die acteert op basis van de gegeven code.[34] BART! heeft een lineair proces, waarbij data van burgers




worden uitgewisseld met overheden, die vervolgens een terugkoppeling geven. In zo'n context kan de technologie worden geïnstalleerd tussen beide partijen. Door de tussenkomst neemt de technologie de compliance voor zijn rekening.

De mate waarin de technologie compliance kan dragen is afhankelijk van de in de technologie geïmplementeerde maatregelen. In eerste instantie zal de technologie vooral ondersteuning bieden,

[33] BART! Uitwerking Richtinggevende vragen "Balans tussen Ethiek en Privacy", Hans Arnold TIGNL 010310
[34] De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Cambridge, Massachusetts; London; Verenigd Koninkrijk: Harvard University Press. Doi:10.2307/j.ctv2867sp

waarna verdere ontwikkeling de verantwoordelijkheden en lasten van burgers en professionals kan afbouwen.

Tot slot, regulerende technologie is niet vanzelfsprekend, omdat zoals hierboven is aangegeven het geheel afhankelijk is van het programmeren en schrijven van code. De juiste code zorgt voor de juiste resultaten, echter onjuiste code zorgen voor foutieve resultaten. Code is in principe stationair en niet flexibel. Het interpreteren van 'open' wettelijke bepalingen is iets wat code niet kan, daarom moet code zo exact mogelijk zijn. AI kan hier uitkomsten bieden, omdat deze technologie gebaseerd is op het weerspiegelen van het menselijke denken, aldus het interpreteren van data. Als het herkennen van persoonsgegevens en context in verschillende vormen (tekst en beeld) mogelijk is, dan kan dat een opmars zijn naar regulerende technologie. In alle gevallen dient de technologie transparant te zijn, zodat professionals door middel van inzicht grip houden op het proces en de uitkomsten. Een transparant AI-systeem is een zogenaamde 'glass box', omdat het doorzichtig (transparant) en inzichtelijk is. Een ondoorzichtige 'black box' is dat niet en zo'n systeem is niet te volgen, waardoor het in het kader van verantwoording en uitlegbaarheid niet wenselijk is.

### 6.7.3 Gebruik van innovatieve technologie

Binnen BART! zullen verschillende technieken en technologieën worden gebruikt die betrekking hebben op verschillende fases van het proces. Dit zijn als het ware de bouwblokken waarmee de verwerkingstechnologie kan worden opgebouwd.

Het eerste bouwblok is het ophalen en inlezen van berichten uit de aangesloten applicaties, hetgeen mogelijk is via 'retrieving messages' technieken zoals scraping. Bij scraping worden berichten 'geschraapt' van het aangesloten platform om vervolgens geanalyseerd te worden op relevantie. Zodoende kan BART! berichten 'schrapen' die relevante onderwerpen bevatten op het gebied van leefbaarheid en veiligheid.

Hierop volgen de stappen datavoorbereiding en data-analyse, waarin de opgehaalde data geanalyseerd zal worden. Gedurende deze stap worden gegevens gefilterd en gesorteerd ten behoeve van de volgende stap.

De derde stap die volgt op de datavoorbereiding en de data-analyse is Machine Learning. Machine Learning is cruciaal om alarmsituaties en onderwerpen te kunnen voorspellen op basis van de voorgeselecteerde data.

Hierna volgt een Complex Event Processor die de data uit de Machine Learning oppakt. De Complex Event Processor clustert berichten van incidenten op basis van variabelen zoals tijd en onderwerp. Op deze manier kunnen meldingen over dezelfde situatie samengevoegd worden om een beter beeld te geven aan de professional.

Tot slot, naar alle waarschijnlijkheid zullen cloud-based databases worden gebruikt om de data in op te slaan zolang dit noodzakelijk is voor de verwerking. De bijbehorende presentatie van de BART!-data zal gegeven worden in een op maat gemaakt dashboard met visualisaties zoals kaarten, woordenwolken, tabellen en grafieken.

# 7. Barrièremodel BART!

Terugkomende op de domeinen binnen BART! en met name de interactieve driehoek uit hoofdstuk zes, zijn de verschillende domeinen in de onderstaande figuur uitgediept. In dit figuur is ook de driehoek te herleiden, omdat het vak samenwerken ‘afspraken en richtlijnen’ tussen burgers, professionals en technologie valt.

Het inbedden van ethiek, privacy en dataprotectie is enkel mogelijk als er voldoende maatregelen worden genomen. In het document zijn de maatregelen ook wel benaderd als barrières tegen onrechtmatigheden. Naast genoemde technische maatregelen in paragraaf 6.5 zijn organisatorische en sociale maatregelen vereist. Organisatorische maatregelen zijn gericht op de taken van de overheidsorganisaties en sociale maatregelen zijn gericht op de burger. Er is beargumenteerd dat het lastig is om door middel van organisatorische en sociale maatregelen de doorvoer van data in en vanuit de technologie te verhinderen. Om die reden is het belangrijk dat er een barrièremodel is met daarin de mogelijkheden om de organisatorische en sociale maatregelen te implementeren in de technologie. Op die manier is er meer grip op het hele proces, van input tot output.

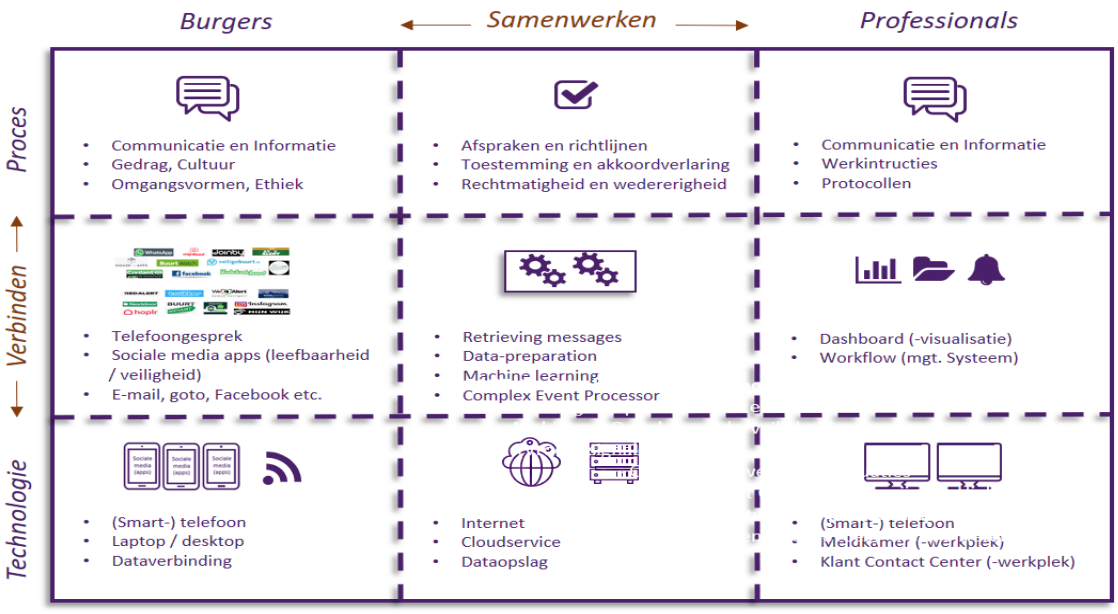
Een barrièremodel kan gebruikt worden om processen in kaart te brengen met hindernissen of voorwaarden. Om bij de volgende processtap te komen moet aan een bepaalde voorwaarde worden voldaan. Deze voorwaarden kunnen in een barrièremodel vormgegeven worden om visueel en procesmatig te tonen welke voorwaarden van belang zijn. Het CCV geeft aan de barrièremodellen voornamelijk te gebruiken voor veiligheidsonderwerpen- en processen. Daarnaast kunnen op deze manier processen in kaart worden gebracht voor allerlei verschillende bedrijfsprocessen.[35]

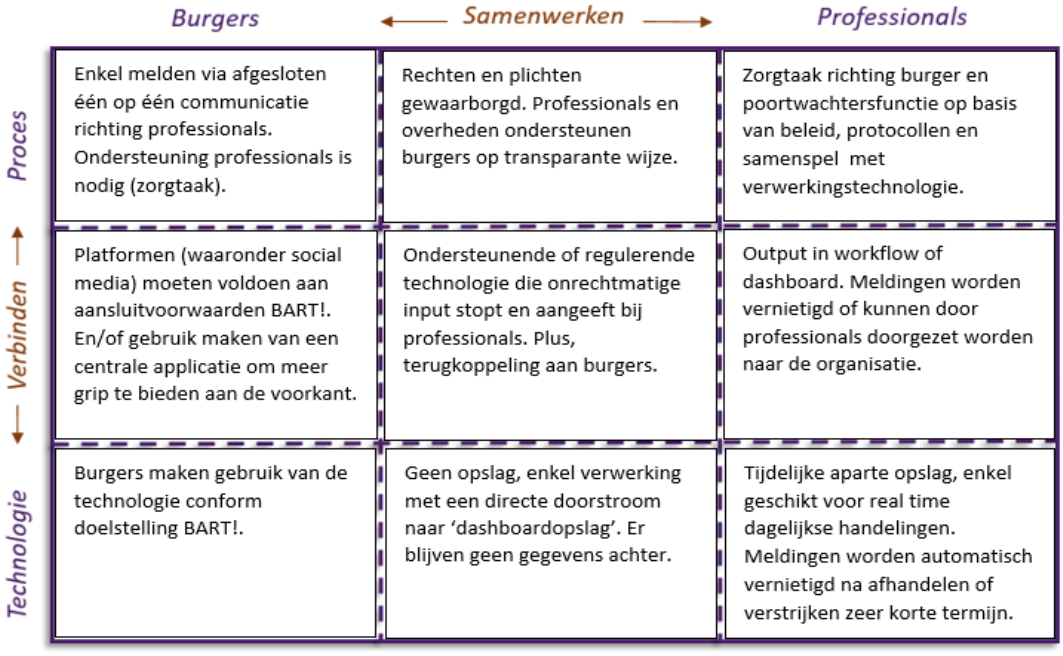
Op deze manier kan het BART!-proces vanuit het perspectief van privacy aangehaald worden. Het proces heeft namelijk te maken met persoonsgegevens waaraan gedurende het proces voorwaarden moeten worden gesteld om onrechtmatige verwerking te voorkomen. Aldus, er moeten barrières geformuleerd worden die onrechtmatigheden tegen gaan. Uiteindelijk kunnen omwille van het waarborgen van ethiek, privacy en dataprotectie de benodigde maatregelen en de processen samengevoegd worden in een barrièremodel. Voor het barrièremodel zal in de volgende paragraaf een opzet worden gegeven die BART! eerst als lineair proces toelicht. In een later stadium kan een barrièremodel worden gevormd als richtlijn voor het eindelijke BART!-ontwerp.

[35] CCV - https://barrieremodellen.nl/

## 7.1 BART! als lineair proces beschouwd

BART! kan lineair worden bekeken, namelijk vanuit een procesmatig oogpunt (eerste rij). Hierbij levert de burger input, waarna het via de verwerking bij professionals terecht komt. Opgemaakt kan worden dat alle partijen (burgers, verwerkingstechnologie en professionals) een ‘fixed position’ innemen. Dat wil zeggen dat het initiatief in eerste instantie altijd bij de burger (melder) ligt en dat op basis van die gegevens de technologie de verwerking uitvoert, waarna de professional aan bod komt. Vanuit dit lineaire proces zijn verschillende barrières beschreven in dit stuk, zie de onderstaande figuren.

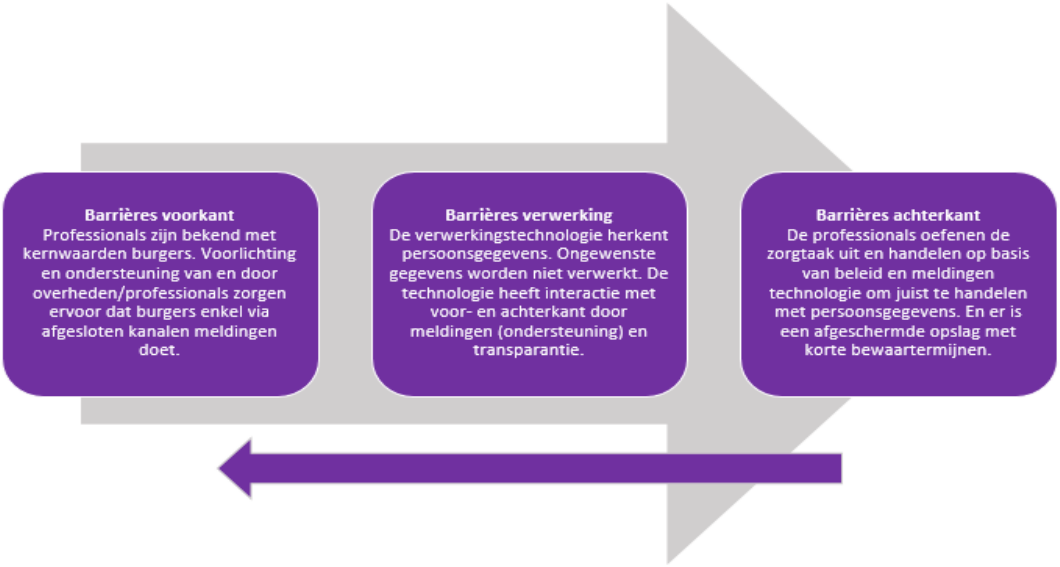


Er zijn twee domeinen die slechts kort worden benoemd in deze figuren, namelijk de platformen (social media en applicaties) en de overheidsorganisaties die aansluiten bij BART!. De eerstgenoemde is een extra factor aan de voorkant van het proces. Zoals het voor burgers niet toegestaan is om persoonsgegevens openbaar te delen is het ook niet gewenst dat bedrijven zoals social mediapartijen over gevoelige gegevens uit meldingen beschikken.

Een risico-inventarisatie van applicaties die aangesloten kunnen worden is daarom onoverkomelijk. Hierbij zal gekeken moeten worden naar de mate van afscherming (encryptie) van de berichten en de opslag daarvan. Een centrale BART!-applicatie kan deze factor tenietdoen en meer grip bieden.

Tot slot, de aangesloten overheidsorganisaties moeten voldoen aan standaarden op het gebied van privacy- en securitynormen met het bijbehorende beleid, protocollen en andere handvatten die professionals ondersteunen om succesvol en juist te werk te gaan. Een afgeschermde dataopslag zoals beschreven in de dit stuk is een vereiste voor de poortwachtersfunctie van de professionals.



# 8. Conclusies en aanbevelingen

BART! Burger Alert Real Time (BART!) is een digitaal meldingsplatform voor een veilige en leefbare buurt. Zaken met én zonder spoed kunnen buurtbewoners 24/7 delen met politie, gemeente en andere bij BART! aangesloten overheidsorganisaties. BART! draagt bij aan de zelfredzaamheid van de burgers, waardoor zij ook zelf acties kunnen ondernemen om de leefbaarheid in wijken te verbeteren. Bij overlast, verdachte situaties of sociale problemen doen burgers een digitale melding en indien nodig onderneemt de politie of de gemeente direct actie. Het doel van BART! is burgers en professionals in hun eigen kracht te ondersteunen en samen te werken aan samenredzaamheid ten behoeve van het verbeteren van een leefbare en veilige woonomgeving. Voor het realiseren van dit doel werkt BART! met persoonsgegevens die alleen worden gebruikt om de doelstelling van BART! te bereiken. Doordat BART! werkt met persoonsgegevens, dient BART! te voldoen aan de privacywetgeving met als doel om burgers controle te bieden over hun eigen opgeslagen persoonsgegevens.

Het inbedden van Ethiek, Privacy en DataProtectie binnen BART! is enkel mogelijk als er voldoende sociale-, organisatorische en technische waarborgen tegen onrechtmatigheden gedefinieerd zijn. Deze waarborgen zijn maatregelen die als barrières tegen onrechtmatigheden functioneren in het BART!-proces. Zowel aan de voorkant, bij de verwerking en aan de achterkant van het proces zijn die barrières nodig om het wederzijds vertrouwen tussen burgers en professionals in BART! te realiseren en persoonsgegevens veilig en juist te gebruiken.

De eerste barrière bevat maatregelen aan de voorkant van het proces. Deze barrière draagt ervoor zorg dat burgers:

1. bekend zijn met de kernwaarden voor burgers die deelnemen aan BART!;
2. alleen leefbaarheids- en veiligheidsoverlast melden via afgeschermde kanalen;
3. vooraf toestemming hebben gegeven voor het gebruik van hun persoonsgegevens in het geval dat dat deze nodig zijn om de gemelde overlast op te lossen.

De tweede barrière betreft de barrière in het midden van het proces rond de verwerkings-technologie. Deze barrière draagt ervoor zorgt dat de technologie:

1. persoonsgegevens/berichten met hatelijke inhoud in meldingen herkent en aangeeft bij professionals en burgers of zelfs automatisch conform privacywetgeving aanpast en doorzet;
2. persoonsgegevens die in strijd zijn met de privacyregels niet verwerkt;
3. kan communiceren en interacteren tussen eerste, derde barrière en/of meerdere barrières die in de toekomst nodig zijn om BART! te laten functioneren (feedback aan burger en professional).

De derde barrière betreft de barrière rond de professionals. Deze barrière draagt ervoor zorg dat de professionals:

1. bekend zijn met de kernwaarden gedefinieerd voor professionals;
2. hun zorgtaak overeenkomstig de AVG en Wpg richting de burger kunnen uitvoeren, waaronder het actief ondersteunen in het borgen van privacy en het uitdragen van rechten van betrokkenen;

3. veilig kunnen werken met persoonsgegevens die gebruikt moeten worden om handelings-perspectieven uit te geven en daarmee als poortwachter functioneren aan het einde van het proces.

BART! maakt het mogelijk aan te sluiten bij de communicatie van burgers in hun buurtgroep. De communicatie verloopt of via verschillende applicaties van derden of via een centrale applicatie. Hierin zal een keuze moeten worden gemaakt, omdat derde partijen zoals sociale media partijen (kanalen waarover burgers veelvuldig communiceren) een risico kunnen opleveren. Strenge aansluitvoorwaarden kunnen dit risico beperken. Eventueel is een combinatievorm ook mogelijk.

BART! technologie faciliteert de communicatie tussen burgers en overheden. Deze technologie zet meldingen enkel door naar juiste overheidsorganisaties op basis van scraping communicatie-platformen. Ondersteunende of zelfs regulerende technologie zet gegevens onttrokken uit de meldingen en bronnen rechtmatig door aan professionals voor communicatie met burgers over de melding. In BART! meldingen zijn informatie en persoonsgegevens permanent technisch gebonden aan de originele context waarbinnen de melding gedaan is. Het gebruik van persoonsgegevens binnen BART! is technisch zo ingericht dat deze alleen maar gebruikt kunnen worden om het vooraf gestelde doel te bereiken. BART!-technologie moet in staat zijn om verschillende soorten persoonsgegevens zoals kentekens en gezichten te onderkennen. Op basis daarvan kan feedback gegeven worden aan burgers of professionals die de doorvoer controleren. De technologie zou op deze manier ook discriminerende/haatdragende termen in tekst en beeld kunnen herkennen, wederom met feedback aan burger en professional.

Overheidsorganisaties betrokken binnen BART! jagen de participatie aan, hierdoor dragen zij een verantwoordelijkheid die zich uit in de zorgtaak van de professional. Zo moet de professional zorgdragen dat er afspraken gemaakt en nageleefd worden met en door de burger. Mocht de burger hierin tekortschieten, dan is de professional de poortwachter die onrechtmatigheden kan signaleren (in samenwerking met de technologie) en herstellen. Het voorkomen van onrechtmatigheden kan alleen als er voldoende barrières zijn rondom de input van burgers.

De professional in het meldkamerproces is binnen het BART!-proces de poortwachter die onrechtmatigheden buitensluit en gewenste zaken doorlaat. De professional krijgt de informatie door uit de verwerkingsunit en kan pas hierna handelingsperspectieven afgeven aan andere professionals en burgers. Burgers onderling kunnen op basis van de terugkoppeling waarin gevoelige gegevens zijn weggelaten met elkaar interacteren.

BART! professionals hebben de plicht om betrokken melders te informeren over de verwerkingen. Deze plicht komt te vervallen als een van de vele uitzonderingsgronden kan worden toegepast door de gemeente of de politie uit respectievelijk de AVG en de Wpg. Daarnaast stellen overheidsorganisaties de betrokkene op de hoogte als er voldaan is aan het verzoek van rectificatie of het wissen van gegevens. Als betrokkene van mening is dat de gegevens niet kloppen, dan kan de betrokkene een schriftelijk verzoek bij de betreffende organisatie indienen waarin wordt aangeven wat er gewijzigd moet worden. De bij BART! aangesloten organisaties hebben het recht een verzoek af te wijzen als het de veiligheid in het geding brengt of anderszins op basis van uitzonderingsgronden.

# 9. Project BART!

## 9.1 BART! samenwerkingsproject

In het project BART! werken politie, gemeente Den Haag, CGI, TNO, TIGNL en burgers samen. Het project BART! onderzoekt de mogelijkheden en vereisten voor een innovatief participatieconcept tussen bewoners, gemeente en politie. Het concept ondersteunt de burger in het werken aan een veilige en leefbare buurt, samen met gemeente en politie. Zo bevorderen we de samenredzaamheid van buurtbewoners. Zie voor meer informatie https://www.bartportal.nl/.

Het participatieconcept bestaat uit functionele, technische en organisatorische modules. We werken aan de ontwikkeling van functionele modules, waaronder het filteren van relevante informatie uit ongestructureerde data van social media, mobiele apps en het gestructureerd aanbieden van deze informatie aan bijvoorbeeld klantcontactcentra of meldkamers. Ook werken we aan een module die interactie tussen de professional en de burgers via social media mogelijk maakt. Denk daarbij aan interactie bij de verdere uitvraag omtrent een incident, het geven van handelingsperspectief (manieren om iets te doen), of het geven van terugkoppeling over de afhandeling. Onder de term social media vallen in de context van BART! ook mobiele apps waarmee burgers berichten aan elkaar kunnen versturen en mobiele apps via groepen burgers ondersteunen in een buurt

## 9.2 Financiering BART!

BART! is mogelijk gemaakt door medefinanciering verstrekt door het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, het Ministerie van Justitie en Veiligheid, de politie, de gemeente Den Haag en de projectpartners TU Delft, TNO, CGI en TIGNL B.V..

# 10. Disclaimer

De informatie in dit rapport is gebaseerd op inzichten en resultaten van het samenwerkingsproject BART!. Het rapport is met grote zorg samengesteld. TIGNL, de project partners en de financiers, kunnen niet verantwoordelijk gehouden worden voor enige onjuiste en/of onvolledige informatie in dit rapport.

# 11. Literatuurlijst


1. Verbeek, P.P. (2014), Op de vleugels van Icarus: hoe techniek en moraal met elkaar meebewegen.
2. Burgers in veiligheid, Marco van der Land, Bas van Stokkom & Hans Boutellier, Vrije Universiteit Amsterdam 2014
3. Rathenau Instituut Rapport Opwaarderen - Borgen van publieke waarden in de digitale samenleving' 06 febr. '17
4. Eindrapport_Big_Data_in_zicht-Nationale_DenkTank_2014.pdf
5. TNO (2015), Privacy beleving op het internet in Nederland.
6. Homo Digitalis 2016 E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne, A.H.J. Schmidt
7. M. J. Bonthuis en E. Duiker, Convenant Gegevensverwerking Meldkamers Uitgave. 20-06-2016, CONCEPT versie 1.19
8. Beleidskader integriteit Politie, Vastgesteld in de Raad van Korpschefs i.o. van 2 en 3 februari 2010
9. Cameratoezicht, Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet Politiegegevens
10. Beroepscode Politie
11. Actief burgerschap Ted van de Wijdeven, Laurens de Graaf, Frank Hendriks, 2013, Tilburgse School voor Politiek en Bestuur
12. De invloed en effecten van sociale samenhang, Astrid Huygen en Free de Meere, April 2018, Verwey Jonker Instituut
13. Meldkamers, februari 2015, Inspectie Veiligheid en Justitie
14. Integriteit van ambtenaren Prof.dr. A.F.A. Korsten en dr. J.I.H.Janssen, Management in overheids-organisaties, Kluwer, 2002.
15. Kamerbrief over rapport privacybeleving op het internet in NederlandDGETM-TM / 15037506
16. Regels inzake de verwerking van politiegegevens kst-30327-3
17. Informatie gestuurd politiewerk, ISBN 978 94 6350 006 7
18. BART! Uitwerking Richtinggevende vragen "Balans tussen Ethiek en Privacy", Hans Arnold TIGNL 010319
19. BART! Ethiek, Privacy en Dataprotectie principes, zie rapport Privacy By Design Hans Arnold TIGNL 010319
20. De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Cambridge, Massachusetts; London; Verenigd Koninkrijk: Harvard University Press. Doi:10.2307/j.ctv2867sp
21. Privacyregulering in theorie en praktijk, J.M.A. Berkvens ; J.E.J. Prins, ISBN9789013040517


**Vergelijkingen artikelen Wbp en Verordening Gegevensbescherming.**

Referentie: Homo Digitalis 2016 E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E Tjong Tjin Tai, G-J. Zwenne, A.H.J. Schmidt,.

## Geraadpleegde Websites

**Overige**

https://www.bartportal.nl/
https://www.gemeente.nu/bestuur/gemeenten-kunnen-geluk-beinvloeden/
https://www.wetten.overheid.nl/
https://www.barrieremodellen.nl/
https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg
https://wetten.overheid.nl/BWBR0022463/2020-01-01- Wet Politiegegevens

**Interessante video presentatie**

https://www.npo.nl/hoe-techniek-en-moraal-met-elkaar-meebewegen/15-04-2014/WO_VPRO_515887

Status exemplaar februari 2020 versie 0.9, redactie, lay-out en opmaak onderhanden werk nog niet definitief afgerond.