

Business-to-government datadelen via een derde. Onderzoek naar een generiek juridisch-technisch data governance raamwerk.

Dr. H.L. Janssen ^{1, 2}

*Bedrijven bezitten gegevens die een (lokale) overheid kunnen helpen een meer accuraat en evidence-based beleid te vormen en uit te voeren. Bestaat er een werkwijze waarop een gemeente toegang kan verkrijgen tot gegevens die bedrijven bezitten, en kunnen gemeenten die vervolgens op verantwoorde wijze verwerken zonder de rechten, belangen en het vertrouwen van de betrokken bedrijven, consumenten en burgers te beperken of te schaden? Op dit moment vindt business-to-government gegevensdeling ('B2G') op beperkte schaal plaats, en voor zover het al gebeurt, geschiedt het veelal op ad hoc basis. Een dergelijke onsystematische toegang tot gegevens is problematisch omdat deze een meer georganiseerde en voorspelbare ondersteuning van accuraat, evidence-based beleid kan belemmeren. De EU-wetgever heeft wetgeving aangenomen (**Data Act**) om B2G een kader te bieden, maar dat biedt nog niet de gewenste duidelijkheid – noch voor gemeenten, noch voor bedrijven.*

*Bedrijven zijn terughoudend met het delen van gegevens, omdat met gegevens economische, technische, politieke en juridische risico's gemoeid zijn. Deze en andere hindernissen zouden deels mogelijk kunnen worden overkomen door het delen van de gegevens te laten verlopen via een derde partij die erop gericht is de gegevensdeling tussen bedrijven en de gemeente op een juridisch correcte wijze en daarmee betrouwbare manier te (laten) delen. Deze derde, die we '**data intermediary**' noemen mag, teneinde een dergelijke dienst aan bedrijven als de gemeente te kunnen bieden, deze gegevens alleen delen volgens een toegankelijk, transparant en handhaafbaar en specifiek op de situatie gericht juridisch data governance regime. De onlangs in werking getreden EU-**Data Governanceverordening** ('DGA') biedt data intermediaries enkele normen, maar nog geen sluitend data governance regime.*

*Omdat er geen sluitende regelgeving is voor een dergelijk data governance regime voor B2G via een data intermediary (B2G3P) dat de rechten en belangen van alle belanghebbenden, met name van hen die hun gegevens beschikbaar stellen, op juridische wijze reguleert, onderzoek ik in deze paper of een **generiek data governance raamwerk** ontwikkeld kan worden, dat juridische, organisatorische en technische voorwaarden die aan een dergelijk raamwerk moeten worden gesteld, op adequate wijze waar kan maken. We concluderen voorlopig het volgende:*

- i. *een geschikt generiek juridisch data governance raamwerk dient de juridische, organisatorische en technische ('**socio-technische**') aard van gegevensdeling tussen bedrijven, lokale overheden en de data intermediary op passende wijze te reguleren;*
- ii. *dat de **EU-wetgeving** enkele grondlijnen maar geen sluitend kader voor een generiek juridisch data governance raamwerk biedt;*

¹ Heleen Janssen is als universitair docent verbonden aan het Instituut voor Informatierecht. Deze working paper werd mogelijk gemaakt met de toekenning van (i) het Digital Urban Citizenship Fellowship (gefinancierd door de gemeente Amsterdam, de Universiteit van Amsterdam en het NIAS/KNAW) en dat werd uitgevoerd bij Netherlands Institute for Advanced Study (NIAS/KNAW), en (ii) de toekenning van een UvA Responsible Digital Transformations Midsize Grant for interdisciplinary research projects (project nummer R.2127.0055) en een in-kind bijdrage van de gemeente Amsterdam. De RDT Midsize Grant werd gedeeld met dr. Thomas van Binsbergen, Faculteit Natuurkunde, Wiskunde en Informatica / Informatics Institute. Met dank aan mr Etienne Valk (IViR, UvA) voor het kritisch meelezen van de paper en voor en het schrijven van § 4.3.2.

² Deze working paper valt onder een Creative Commons naamsvermelding 4.0 [Internationaal-licentie](#).

- iii. dat **bestaande wetgeving** op coherente en consistente wijze moet worden toegepast maar dat dit **rechtsonzekerheid** met zich meebrengt voor lokale overheden; en
- iv. dat bij het ontwikkelen van een generiek juridisch data governance raamwerk een effectieve mix van juridische, organisatorische en technische (**'socio-technische'**) **aspecten moet worden geadresseerd en dat daarvoor passende socio-technische mechanismen** moeten worden ontworpen.

Deze working paper beschrijft, analyseert en evaluaart i – iv.

Inhoudsopgave

1. INLEIDING	4
1.1 B2G IN DE PRAKTIJK	4
1.2 KAN EEN 'DATA INTERMEDIARY' B2G IN GEMEENTELIJKE CONTEXT VOORUITHELPEN?	6
1.4 WAT STAAT ER OP HET SPEL?	8
1.5 DOEL: NAAR EEN GENERIEK JURIDISCH RAAMWERK VOOR B2G VIA EEN DATA INTERMEDIARY	10
2. B2G	11
2.1 ECONOMISCH-POLITIEKE OVERWEGINGEN BIJ B2G IN GEMEENTELIJKE CONTEXT	11
2.2 GEMEENTELIJKE OVERWEGINGEN	12
2.2.1 'Publieke taak'	13
2.2.2 Vrijwillige en verplichte B2G	13
2.2.3 Juridische, technische en organisatorische mechanismen	14
2.2.4 Burger- en maatschappelijk perspectief	14
2.3 OVERWEGINGEN VAN BEDRIJVEN	15
2.3.1 Zorgen	15
2.3.2 Kansen	16
2.4 VOORGESTELDE STRATEGIEËN VOOR ONTSLUITING VAN GEGEVENS	16
2.4.1 Privacy Enhancing Technologies	16
2.4.2 Differentiatie in het type informatie dat wordt gedeeld	17
2.4.3 Aanvullende strategieën	18
3. WETTELIJK KADER BIJ B2G	19
3.1 FUNDAMENTELE RECHTEN	20
3.2 ALGEMENE VERORDENING GEGEVENSBESCHERMING	20
3.3 AI-VERORDENING	22
3.4 WET BESCHERMING BEDRIJFSGEHEIMEN	23
3.5 WET OPEN OVERHEID	23
3.6 OPEN DATA RICHTLIJN EN WET HERGEBRUIK OVERHEIDSINFORMATIE	23
3.7 ALGEMENE WET BESTUURSRECHT	24
3.8 DATA VERORDENING	25
4. DE DATA INTERMEDIARY	26
4.1 DATA GOVERNANCE	27
4.1.1 Het data governance regime	27
4.1.2 Overwegingen bij het data governance regime	28
4.2 UITVOERING	30
4.2.1 Vastlegging en opslag van gegevens	31
4.2.2 Gegevensverwerking en -deling	32
4.2.3 Transparantie van de gegevensverwerking	33
4.3 WETTELIJK KADER BIJ B2G VIA EEN DATA INTERMEDIARY (3P)	34
4.3.1 Data Governance act	34
4.3.2 Juridische statuut van de data intermediary	35
4.4 UITDAGINGEN BIJ GEGEVENSDELING IN B2G VIA EEN DATA INTERMEDIARY	37
5. B2G3P-ASPECTEN DIE IN EEN GENERIEK JURIDISCH RAAMWERK AANDACHT BEHOEVEN	37

1. Inleiding

Gemeenten zijn verantwoordelijk voor diverse publieke taken. Het kan gaan om dienstverlening aan burgers of bedrijven, met het oog op de verbetering van de leefomgeving, om initiatieven rondom innovatie in de stad aan te jagen, om verkeersknelpunten op te lossen, om de luchtkwaliteit en de gezondheid van burgers te verbeteren, om zorgverlening te leveren waar het noodzakelijk is, om de stad toegankelijker te maken voor fietsers, om kwetsbare grachten te beschermen of om maatregelen te nemen in het kader van het oplossen van afvalproblemen of het borgen van de fysieke veiligheid in de openbare ruimte. Teneinde passend beleid voor deze taken te ontwikkelen heeft de gemeente accurate informatie nodig. Bij het ontwikkelen van beleid en het uitvoeren van taken willen gemeenten zoveel mogelijk *evidence-based* te werk gaan, en daarnaast beslissingen nemen die op accurate informatie gebaseerd zijn. In de huidige, snel digitaliserende samenleving lijkt *evidence-based* gemeentelijke beleidsvorming in toenemende mate afhankelijk te worden van de toegang tot digitale gegevens die in veelal in handen zijn van bedrijven omdat zij informatie bezitten over bijvoorbeeld hetgeen zich afspeelt in de openbare ruimte.

Bij het toegankelijk maken van gegevens afkomstig uit bedrijven voor gemeenten is het concept van "Business-to-Government (B2G) gegevensdeling" relevant.³ Dit concept verwijst naar de uitwisseling van gegevens van de particuliere sector (ondernemingen, verenigingen, stichtingen, enz.) met de publieke sector (centrale of lokale overheden, steden, regio's, enz.).⁴ Het idee achter B2G is dat met het samenbrengen van gegevens uit verschillende bronnen uit de particuliere sector nieuwe waarden en inzichten kunnen worden gecreëerd die waardevol kunnen zijn voor, in het geval van B2G, de publieke sector. Gemeentelijke toegang tot bedrijfsgegevens geschiedt nu veelal op basis van publiek-private afspraken tussen de gemeente en bedrijven; hierin spelen contracten veelal hoofdrol. Soms komt het voor dat de gemeente toegang verkrijgt wanneer die toegang een voorwaarde is voor acceptatie in een aanbestedingsprocedure of voor een vergunning. De praktijk wijst uit dat B2G op dit moment vaak op een ongestructureerde, *ad-hoc* manier gebeurt.

1.1 B2G in de praktijk

De "dataficatie"⁵ van de digitale samenleving – het omzetten van menselijke handelingen in data zodat ze verhandeld of ingezet kunnen worden om menselijk gedrag te monitoren en te sturen – heeft een

³ Het concept van "B2G-gegevensuitwisseling" is ook een van de vier Europese concepten voor gegevensuitwisseling die door de Europese Unie zijn ontwikkeld om structuur te geven aan de Europese gegevens economie (de drie andere zijn "Business-to-Business – B2B", "Government-to-Business – G2B" en "Government-to-Government – G2G" gegevensuitwisseling- zie de Mededeling van de Europese Commissie (2020) "[Een Europese strategie voor data](#)" (COM (2020) 66final).

⁴ A. Petel. 'Chapter 5 of the Data Act – What is the European concept of "B2G data sharing" in the Data Act proposal?', Data Act Blog Post Series KU Leuven (21 juni 2022).

⁵ Term gemunt door J. Van Dijck, in 'Datafication, dataïsm and dataveillance: Big Data between scientific paradigm and ideology' (2014) *Surveillance and Society* 12(2) 197.

ongekend potentieel opgeleverd voor bedrijven⁶ bij het verkrijgen van toegang tot een schat aan data. Op basis van deze gegevens kunnen zij uiteenlopende bedrijfsmodellen baseren, terwijl overheden deze gegevens kunnen gebruiken voor het ontwikkelen en uitvoeren van meer accuraat en meer *evidence-based* publiek beleid.

Voor gemeenten lijkt toegang tot groeiende hoeveelheden gegevens niet op te gaan. Zij worden in toenemende mate geconfronteerd met belemmeringen wanneer zij toegang willen tot gegevens die in handen zijn van bedrijven. Bedrijven die gegevens bezitten hebben sterke juridische, technische, politieke en economische drijfveren om zich te verzetten tegen het delen van gegevens, ook met overheden. Bedrijven kunnen zich beroepen op hun grondrecht op vrijheid van beroep en bedrijf en de vrijheid van ondernemerschap. Daarnaast kunnen ze wijzen op de bescherming van persoonsgegevens in de Algemene Verordening Gegevensbescherming (AVG) die het delen van persoonsgegevens die zij bezitten, aan voorwaarden bindt, of op de bescherming van handelsgeheimen of intellectuele eigendomsrechten. Ook leeft bij diverse bedrijven de angst met het delen van data commerciële kansen mis te lopen, of dat het delen van gegevens de reputatie van een bedrijf kan schaden. Daarnaast kunnen zorgen over kosten die met gegevensdeling gepaard kunnen gaan de toegang van gemeenten tot gegevens in bezit van bedrijven effectief blokkeren.

De weigering van bedrijven om informatie te delen kan van invloed zijn op de nauwkeurigheid, effectiviteit en tijdigheid van de ontwikkeling en uitvoering van gemeentelijke, publieke taken, en daarmee op de leefbaarheid van de stad, of het leven van burgers negatief beïnvloeden, terwijl informatie die aangeeft waar problemen zich waarschijnlijk voordoen al in de gegevens van bedrijven aanwezig kan zijn. Zo kon bijvoorbeeld MasterCard in de afwikkeling van de Covid-19 pandemie op basis van betalingen in winkels in bepaalde wijken in Londen met redelijke zekerheid voorspellen welke wijken niet langer zouden moeten investeren in het behoud van winkelcentra. Dit stelde de gemeente in staat meer accurate keuzes te maken ten aanzien van haar investeringen en steun die nodig was voor behoud van werkgelegenheid in deze wijken.⁷

Meer algemeen lijkt het groeiende bezit van en controle over gegevens door de particuliere sector een consoliderend beweging te vertonen, die de waarde en de waardecreatie van gegevens verplaatst van de publieke sfeer naar de particuliere sector. Hierdoor wordt het transformatieve potentieel – het interpreteren en het relevant maken van gegevens voor het algemeen belang en daarmee voor de publieke sector, inclusief gemeenten en burgers – in toenemende mate beperkt.

Het perspectief van burgers in B2G vraagt om diverse redenen aandacht. Niet alleen kunnen burgers profiteren wanneer de gemeente toegang krijgt tot gegevens via B2G om bijvoorbeeld verkeersknelpunten of luchtvervuiling op bepaalde locaties op te lossen. B2G kan ook gevolgen hebben voor de fundamentele rechten van burgers. Gemeentelijke toegang tot en het gebruik van gegevens

⁶ In deze onderzoekspaper wordt gesproken over bedrijven, maar het kan ook gaan over andere organisaties in de particuliere sector, zoals coöperaties, non-gouvernementele belangenorganisaties, private onderzoeksinstituten, etc.

⁷ “Mastercard stelde de gemeente Londen in staat een beter geïnformeerde begrotingsplanning op te stellen, de uitbetaling van hulp te optimaliseren en prioriteit te geven aan investeringen ter ondersteuning van degenen die het zwaarst getroffen zijn door de pandemie”, A. Kover, ‘The gift of clarity: Data-driven insights help governments shape relief efforts wisely’ (2020), <<https://www.mastercard.com/news/perspectives/2020/the-gift-of-clarity-data-driven-insights-help-cities/>>, bezocht op 1 april 2024.

die werden verkregen van bedrijven kan risico's inhouden voor het recht op bescherming van persoonsgegevens van burgers of voor het recht om niet gediscrimineerd te worden. De kans bestaat dat een gemeente niet precies weet wat voor gegevens zij precies ontvangt en welke specifieke discriminatierisico's aan het gebruik van die gegevens verbonden zijn. Zij creëerde de gegevens immers niet zelf, dat gebeurde elders, buiten het zicht van de gemeente. Wanneer gegevens verkregen uit B2G worden verkregen en gebruikt, moet de gemeente zich van zulke risico's voor burgers steeds bewust zijn. Een gemeente kan bijvoorbeeld een impact assessment ten aanzien van het voorgenomen gebruik en de te verwerken gegevens uitvoeren.⁸ Wanneer de gemeente dit nalaat, kan dat diverse gevolgen hebben, waaronder uitkomsten die het verlies van vertrouwen van burgers en bedrijven in het vermogen van lokale overheden om hun publieke taken te vervullen.

Binnen deze kritieke en complexe context van 'gemeentelijke' B2G rijst de vraag of en op welke wijze B2G dan wel op een verantwoorde manier zou kunnen worden gerealiseerd zodat de publieke sector, en in de context van dit project, gemeenten, kunnen profiteren van het hiervoor genoemde transformatieve potentieel van B2G, en van meer accurate informatie die kan worden gebruikt voor de vervulling van diverse publieke taken. Van cruciaal belang is dat in B2G de rechten en belangen van bedrijven die hun gegevens ter beschikking stellen en burgers (voor zover hun rechten en belangen betrokken zijn in een specifieke B2G-gegevensdeling) steeds worden nageleefd.

1.2 Kan een 'data intermediary' B2G in gemeentelijke context vooruithelpen?

In dit project wordt onderzocht welke knelpunten zich rondom rechten en belangen in B2G in gemeentelijke context kunnen voordoen, en of methoden denkbaar zijn die, afhankelijk van het type knelpunten dat in een concrete situatie speelt, alsnog kunnen bijdragen aan het tot stand brengen van B2G. Eén van de methoden die deze rechten en belangen mogelijk kan borgen, is een methode waarbij B2G niet direct tussen bedrijven en een gemeente plaatsvindt, maar waarbij deze verloopt via een onafhankelijke derde partij. Dit project stelt voor het concept van de '*data intermediary*', een opkomend maar zich snel verbreidend concept⁹ dat mogelijk dienstbaar is om de hiervoor geschetste problematiek (deels) het hoofd te bieden.

Algemeen en in de kern fungeren data intermediaries als 'gegevensbemiddelaar' tussen degenen die hun gegevens beschikbaar willen stellen enerzijds en ontvangers die deze gegevens willen gebruiken anderzijds.¹⁰ De data intermediary beheert de gegevens op een specifiek voorgeschreven wijze, die veelal wordt neergelegd in een 'data governance regime'.¹¹ Het data governance regime van een data intermediary heeft tot doel degenen die hun data beschikbaar stellen en daarmee een zekere mate

⁸ Dit kan een Data Protection Impact Assessment zoals voorgeschreven door art. 35 van de Algemene Verordening Gegevensbescherming (AVG) zijn, of een mensenrechten impact assessment wanneer van een bedrijf door AI-gegenereerde gegevens worden verkregen (beide zijn gericht op de veiligheid van mensen), of een veiligheids impact assessment (dat eerder is gericht op de veiligheid van systemen).

⁹ J. Powar, H. Janssen, R. Cloethe, J. Singh, From policy to practice in data governance and responsible data stewardship: system design for data intermediaries, FAccT '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency, p. 2491–2504, <https://doi.org/10.1145/3715275.373216>.

¹⁰ H. Janssen & J. Singh, Data Intermediary (2022) Internet Policy Review (11) 1, 9.

¹¹ H. Janssen & J. Singh, Data Intermediary (2022) Internet Policy Review 11, 1, 9.

van zeggenschap over hun gegevens verliezen, vertrouwen te bieden over hoe die gegevens zullen worden opgeslagen, verwerkt en gebruikt.¹²

Een data intermediary zal in de kern in staat moeten zijn effectieve maatregelen te nemen om de rechten en belangen van betrokken bedrijven te beschermen door bijvoorbeeld niet de brongegevens van alle bedrijven te delen, maar in plaats daarvan een aggregaat van een analyse over gegevens van één of meer bedrijven te delen met een gemeente zodat de in het bestand aanwezige bedrijfsgeheimen of persoonsgegevens niet worden gedeeld. Ook kunnen voor een data intermediary, afhankelijk van haar rechtsvorm, mogelijkheden worden onderzocht om belanghebbenden zoals burgers burgers adviesrechten of wellicht inspraak te geven in de besluitvorming ten aanzien van te analyseren gegevens. Daarnaast zou een data intermediary vanwege haar onafhankelijke rol mogelijk toegerust kunnen worden met juridische en wellicht technische mechanismen om conflicten tussen de rechten en belangen van bedrijven die hun gegevens beschikbaar stellen en de ontvangende partij – hier de gemeente – zoveel mogelijk proberen te voorkomen of op te lossen.

Het concept van de data intermediary is niet nieuw.¹³ Een data intermediary faciliteert nu al gegevenstoegang en-gebruik in deels vergelijkbare situaties.¹⁴ Wanneer twee of meer bedrijven met behulp of onder regie van een data intermediary overgaan tot het delen van data met elkaar (B2B). Zo hebben vliegtuigmaatschappijen grote belangen bij het veilig houden van de eigen vloot, maar levert de eigen vloot te weinig data om mogelijke materiaalrisico's tijdig te detecteren.¹⁵ Wanneer 100 vliegtuigmaatschappijen bereid zijn dit soort data over de eigen vloot te delen, ontstaat een interessante bron van informatie die kan leiden tot betere en meer accurate inzichten. De commerciële belangen die aan dit type gegevens kleven verhinderen echter dat bedrijven deze informatie met anderen delen. De Laat en Gommans et al. stelden voor een data intermediary te ontwikkelen die, als onafhankelijke derde, van alle in de B2B betrokken maatschappijen als enige toestemming zou krijgen om gegevens van deze maatschappijen te analyseren en risico's te identificeren. Vervolgens werden niet de data zelf gedeeld, maar uitkomsten van de risico-analyses van het materiaal, zodat alle maatschappijen weten waarop ze moeten letten bij het garanderen van veilige vluchten.¹⁶ Het concept 'data intermediary' op uiteenlopende manieren ingevuld.¹⁷

¹² H. Janssen & J. Singh, Data Intermediary (2022) Internet Policy Review (11) 1, 9.

¹³ Sylvie Delacroix and Neil D Lawrence. 2019. Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance. International Data Privacy Law 9, 4 (Nov. 2019), 236–252; Todd Hartman, Helen Kennedy, Robin Steedman, and Rhianne Jones. 2020. Public Perceptions of Good Data Management: Findings from a UK-based Survey. Big Data & Society 7, 1 (2020); Marina Micheli, Marisa Ponti, Max Craglia, and Anna Berti Suman. 2020. Emerging Models of Data Governance in the Age of Datafication. Big Data & Society 7, 2 (July 2020).

¹⁴ T. Araujo, J. Ausloos, W. van Atteveldt, F. Loecherbach, J. Moeller, J. Ohme, D. Trilling, B. van de Velde, C. De Vreese, and K. Welbers. 2022. OSD2F: An Open-Source Data Donation Framework. Computational Communication Research 4, 2 (2022), 372–387; The W3C Solid Community Group. 2016. The Solid Project. <https://solidproject.org/>; UK Government. 2021. Check the Long Term Flood Risk for an Area in England. <https://www.gov.uk/check-long-term-flood-risk>; F. Monge, S. Barns, R. Kattel, and F. Bria. 2022. A New Data Deal: The Case of Barcelona. Working / Discussion Paper 2022/02. UCL Institute for Innovation and Public Purpose, London, UK. <https://www.ucl.ac.uk/bartlett/public-purpose/publications/2022/feb/new-data-deal-case-barcelona>.

¹⁵ C. De Laat e.a., 'Data for logistics for logistics data' (2017) <<https://dl4ld.nl>> bezocht op 27 maart 2024.

¹⁶ C. De Laat e.a., 'Data for logistics for logistics data' (2017) <<https://dl4ld.nl>> bezocht op 27 maart 2024.

In de context van B2G met de gemeente zou een data intermediary bijvoorbeeld de toegang tot bedrijfsgegevens kunnen faciliteren door de gemeente beperkte toegang te geven – waarbij niet de ruwe, onbewerkte data worden gedeeld, maar alleen specifieke, geaggregeerde informatie die de gemeente nodig heeft om de beleidsontwikkeling en uitvoering van beleid meer *evidence-based* te maken en te verbeteren. Het belangrijkste doel van een data intermediary is steeds het op zodanige wijze beheren van de gegevens dat degenen die hun gegevens beschikbaar stellen een zekere mate van vertrouwen hebben in de wijze waarop hun gegevens toegankelijk zullen worden gemaakt en gebruikt. In de context van gemeentelijke B2G houdt dit bijvoorbeeld in dat de data intermediary onderzoekt of alternatieve, meer indirecte vormen van gemeentelijke toegang tot bedrijfsgegevens die minder of geen risico voor het bedrijf met zich meebrengen voorhanden zijn.

Wat de regeling van het eerdergenoemde data governance regime van de data intermediary betreft, rijst in de eerste plaats de vraag aan welke wettelijke voorwaarden en verplichtingen het *data governance regime* om B2G tot stand te brengen, minimaal moet voldoen om ervoor te zorgen dat B2G met een aanvaardbaar risico voor alle betrokken partijen tot stand wordt gebracht. In de tweede plaats komt de vraag aan op welke voorwaarden en regels de data intermediary *zelf* moet voldoen om B2G tot stand te brengen die binnen de geldende wettelijke regels past. In de tweede plaats komt de vraag op aan

Een juridisch perspectief op de mogelijkheden en beperkingen van B2G via een data intermediary is tot op heden nauwelijks kritisch onderzocht, behalve in het Google/Toronto-project. Dit betrof een *use case* waarin Google de rol van data intermediary op zich nam van waaruit Google in de eerste plaats vanuit een eigen, commercieel perspectief B2G ten behoeve van het publieke, algemeen belang van de stad Toronto faciliteerde.¹⁸ Dit liep uit op een mislukking vanwege het feit dat Google de rol vervulde vanuit zijn commerciële perspectief en daarmee het publieke belang uit het oog verloor.

Het is cruciaal het data governance regime ten behoeve van B2G zodanig in te richten dat de rechten en belangen van bedrijven die hun gegevens ter beschikking stellen worden nageleefd en gerespecteerd en dat de publieke doelstelling bij de gemeente bij deelname aan B2G voorop staat. De wijze waarop de data intermediary zou moeten worden ingericht en de eisen waaraan het data governance regime zou moeten voldoen zullen voorwerp van vervolgonderzoek zijn van dit onderzoeksproject.

1.4 Wat staat er op het spel?

Enkele urgente redenen nopen tot het ontwikkelen van een passend juridisch kader rondom gemeentelijke B2G. Het betreft motivaties en ontwikkelingen op gemeentelijk en nationaal niveau, en op EU-niveau. Het huidige juridisch kader rond B2G via een data intermediary kent juridische onzekerheden. Op B2G is een groot aantal wetten en regelingen van toepassing; of deze steeds op coherente wijze worden toegepast bij een specifieke B2G is onduidelijk. Het vraagt expertise die niet bij elke gemeente voorhanden is. Ook is nog niet duidelijk of wetgeving ontbreekt, of dat inconsistenties tussen de toepasselijke wetten naar voren komen in B2G. Gemeenten kunnen met

¹⁸ T. Scassa, 'Sharing data in the platform economy: a public-interest argument for access to platform data' (2017) UBC Law Review 50(4).

beperkte publiekrechtelijke en privaatrechtelijke instrumenten B2G initiëren, maar hebben geen bevoegdheden formele wetgeving tot stand te brengen om leemten of inconsistenties in de wetgeving rondom B2G aan te pakken. Deze juridische onzekerheden rondom gemeentelijke B2G worden waarschijnlijk niet op korte termijn weggenomen. Bovendien blijft onlangs aangenomen Europese wetgeving – de Data Governance Verordening en de Data Verordening (waarover hierna meer) erg abstract voor wat betreft gemeentelijke B2G.¹⁹

Vervolgens spelen diverse politiek-economische redenen waardoor de gemeente in de digitaliserende omgeving een minder sterke rol heeft als het gaat om de toegang tot en het gebruik van gegevens in de particuliere sector. Dit is onder meer een gevolg van privatisering van diverse diensten die traditioneel door de publieke sector werden vervuld. Veel technologieën waarmee gegevens worden gegenereerd zijn doorgaans ontworpen en ontwikkeld door bedrijven en in mindere mate door gemeenten.²⁰ Daarmee definiëren en bepalen bedrijven vaak de praktische-, technische- en kennisvoorwaarden voor de gegevensverwerking en het beheer van die gegevens, hetgeen hen feitelijke beslismacht geeft over welke gegevens worden vastgelegd, opslagen, geduid, geaggregeerd of overgedragen,²¹ en niet de overheid.

Daarnaast heeft de structurele en grootschalige verzameling van gegevens door (BigTech) bedrijven gevolgen voor het machtsverhouding tussen de gemeente en bedrijven; bedrijven zijn daardoor beter dan de gemeente geïnformeerd over welke problemen zich bijvoorbeeld in de openbare ruimte in een gemeente voordoen.²² Via netwerken, gegevensstromen en infrastructuren waarover zij vaak exclusief controle uitoefenen kunnen zij een informatievoorsprong opbouwen ten opzichte van de gemeente. Gemeenten hebben daarmee minder toegang tot gegevens, althans niet in die omvang en op dat detailniveau.²³ Deze voorsprong beïnvloedt het (onder)handelingsperspectief van de gemeente bij het verkrijgen van toegang tot die gegevens. Bedrijven zijn vanwege hun informatiepositie beter in staat eenzijdig voorwaarden te stellen aan gemeentelijke toegang tot gegevens.²⁴ En: indien en voor zover bedrijven al gegevens delen met de gemeente, beschikken gemeenten lang niet altijd over de middelen (kennis, expertise, opslagcapaciteit, ervaring met de uitvoering van analyses) om de ontvangen gegevens te verwerken en te gebruiken, waarvoor ze eveneens afhankelijk zijn (en blijven) van actoren uit de particuliere sector.²⁵

¹⁹ B. Lazarotto, S. Stalla-Bourdillon, P. R. Trigo Kramasac. Giving EU data governance law a second life? From rebranding to real-world impact. Social Sciences Research Network (SSRN) (10 December 2025).

²⁰ In de gevallen waarin gemeenten zelf innoveren op digitale technieken is dat vaak een reactie op technologieën ontworpen door bedrijven. De gemeente Amsterdam (en een aantal andere Europese steden) was eerder actief in het DECODE project dat beoogde burgers meer zeggenschap te geven over hun gegevens zie <<https://decodeproject.eu>> bezocht op 2 april 2024. Zie ook C. Nevejan, City science for urban challenges, Pilot assessment and future potential of the City science initiative 2019 – 2020, 46 <https://openresearch.amsterdam/image/2020/12/8/cahier2_city_science.pdf>.

²¹ J. Mercille, Inclusive smart cities: beyond voluntary corporate data sharing (2021) Sustainability 8135, 1.

²² H. Janssen, L.W. Verboeket en A.Meiring, Gemeentelijke grip op private sensorgegevens. Juridisch kader voor het gemeentelijk handelingsperspectief bij de verwerking van private sensorgegevens in de openbare ruimte. Rapport van een onderzoek in opdracht van de gemeente Amsterdam (juli 2023) <https://www.ivir.nl/publicaties/download/Gemeentelijke_grip_op_private_sensorgegevens.pdf> bezocht op 27 maart 2024.

²³ Janssen e.a. (2023).

²⁴ T. Scassa, Sharing data in the platform economy: a public-interest argument for access to platform data (2017) UBC Law Review 50(4) 1017.

²⁵ Z. Allam, Cities and the Digital Revolution, Aligning Technology and Humanity. Palgrave Macmillan, Londen 2020.

De EU heeft “digitale soevereiniteit” hoog op haar politieke langetermijnstrategie geplaatst.²⁶ Digitale soevereiniteit is erop gericht het huidige machtsverevenwicht over toegang tot en controle over het gebruik van informatie tussen multinationale technologiebedrijven enerzijds en burgers en particuliere en openbare instellingen (waaronder nationale, Europese en lokale overheden) anderzijds, te doen verschuiven. Een belangrijk doel dat met die verschuiving wordt nagestreefd is het verminderen van de kwetsbaarheid van publieke instellingen, op alle niveaus en in alle sectoren, ten opzichte van (grote) bedrijven die de data-infrastructuren en gegevens over een ongekend scala aan menselijke en maatschappelijke activiteiten beheren en controleren. Dit onderzoeksproject onderzoekt vanuit juridisch perspectief of B2G via een derde partij een bijdrage kan leveren aan deze beleidsprioriteiten.

Daarnaast is een punt bereikt waarop het gebrek aan rechtvaardig gegevensbeheer onder democratische controle, dat beantwoordt aan de normatieve verwachtingen van moderne democratieën, niet langer een theoretische kwestie is die slechts in abstracto kan worden bestudeerd. De gemeente Amsterdam heeft onderzoeksprojecten geïnitieerd waaraan ook het Instituut voor Informatierecht van de Universiteit van Amsterdam deelnam, omdat de gemeente worstelt met ernstige hindernissen die haar beletten haar mandaat te vervullen.²⁷ Dit probleem speelt ook in andere steden in Nederland en Europa.²⁸

In de derde plaats bestaat een dringende behoefte aan specifiek juridisch onderzoek naar de mogelijkheden en beperkingen rondom B2G via een data intermediary. De onlangs aangenomen DGA en Data Act (en andere relevante wetten waaronder de Kunstmatige Intelligentie Verordening, de ‘AI-Verordening’) roepen substantiële en complexe vragen op over interpretatie, implementatie en handhaving, vergelijkbaar met de vragen die werden opgeworpen ten tijde en ver na de invoering van de Algemene Verordening Gegevensbescherming (AVG). De hoeveelheid wetenschappelijk werk rond de AVG geeft de reikwijdte en diepgang aan van het academisch onderzoek dat nodig is met betrekking tot B2G en de daaraan gekoppelde publiek-private regelingen voor het gegevensbeheer. Het geval van de AVG heeft aangetoond dat interdisciplinair wetenschappelijk onderzoek met nauwe betrokkenheid van belanghebbenden vaak de beste, en soms de enige manier is om dergelijke complexe uitdagingen op het snijvlak van wetgeving, technologie en samenleving te onderzoeken en aan te pakken.

1.5 Doel: naar een generiek juridisch raamwerk voor B2G via een data intermediary

Dit project loopt vooruit op ontwikkelingen in de EU waar wordt onderhandeld over de belangrijkste contouren van de regelgeving, die het probleem en de oplossingen daarbij voor het komende decennium definieert. Het project onderzoekt of de regelgevers op het juiste spoor zitten. De hoofdvraag die ik in het project wil beantwoorden is of het mogelijk is een juridische ‘blauwdruk’ te ontwikkelen voor een data intermediary die de uitdagingen en valkuilen bij B2G op gemeentelijk

²⁶ Mededeling van de Europese Commissie (2020) ["Een Europese strategie voor data"](#) (COM (2020) 66final).

²⁷ Janssen e.a. (2023).

²⁸ D. van Barneveld, C. Corver en A. Yeh, Sensoren en de rol van gemeenten. VNG Realisatie Whitepaper (maart 2018); T. Marsic, ‘When billboards stare back. How cities can reclaim the digital public sphere’, Nesta – Cities Coalition for Digital Rights (mei 2022); H. Janssen, L.W. Verboeket en A. Meiring, Gemeentelijke grip op private sensorgegevens. Juridisch kader voor het gemeentelijk handelingsperspectief bij de verwerking van private sensorgegevens in de openbare ruimte. Rapport van een onderzoek in opdracht van de gemeente Amsterdam (juli 2023)

<https://www.ivir.nl/publicaties/download/Gemeentelijke_grip_op_private_sensorgegevens.pdf> bezocht op 27 maart 2024.

niveau kan faciliteren. Deze blauwdruk moet op een zo concreet mogelijk niveau de minimale elementen formuleren die het data governance regime voor de data intermediary nodig heeft. Het project gaat met name *niet* in op het gebruik van gegevens uit B2G voor strafvorderlijke- of fraudebestrijdingsdoelstellingen van de gemeente.²⁹

In deze paper worden onderzoeksbevindingen weergegeven rondom B2G (hoofdstuk 2) en volgt een overzicht van waarschijnlijk relevante, in alle sectoren van toepassing zijnde wetgeving (hoofdstuk 3) en een verkenning van de eigenschappen van data intermediary (hoofdstuk 4). Het paper sluit af met een inventarisatie van onderzoeksrichtingen die noodzakelijk zijn bij het ontwikkelen van de juridische blauwdruk voor B2G via een data intermediary (hoofdstuk 5).

Het onderzoek is gebaseerd op een analyse van relevante wetgeving, jurisprudentie, wetenschappelijke literatuur, beleidsrapporten en kwalitatieve, semigestructureerde interviews met medewerkers binnen de gemeente en in het bedrijfsleven, en met personen die als data intermediary ervaring hebben. Bij het Netherlands Institute for Advanced Study van de Koninklijke Nederlandse Akademie van Wetenschappen en Kunsten (NIAS/KNAW) is een Workshop georganiseerd over de juiste interpretatie van het toepasselijke juridische kader (9 mei 2023).

2. B2G

Om de doelstellingen van B2G te begrijpen, en de aarzelingen van bedrijven daaraan mee te werken te doorgronden, is het belangrijk om bij de bredere technologische en maatschappelijke context van het debat een beeld te krijgen. Het onderzoek dat bij het NIAS werd verricht zag met name op een verdieping van deze beweegredenen en de maatschappelijke context. In dit hoofdstuk worden enkele economisch-politieke overwegingen die de groeiende aandacht voor B2G rechtvaardigen belicht. Daarna volgen wat meer gedetailleerde overwegingen rondom B2G vanuit gemeentelijk perspectief, alsook die vanuit het perspectief van een bedrijf en een burger. Vervolgens worden het huidige juridische kader voor B2G en de toekomstige gegevenswet (zoals voorgesteld in 2022) geïntroduceerd. Dit hoofdstuk sluit af met enkele praktische benaderingen van manieren waarop sommige uitdagingen van B2G tot nu toe zijn overwonnen.

2.1 Economisch-politieke overwegingen bij B2G in gemeentelijke context

Technische vooruitgang in combinatie met kostenreductie bij het vergaren en opslaan van gegevens heeft veel bedrijven in staat gesteld om steeds grotere hoeveelheden gegevens vast te leggen en te gebruiken voor eigen gewin. Airbnb informatie over de bezetting van woningen, Bookings gegevens over de bezetting van hotels en restaurants of Uber gegevens over gemaakte reizen en gereden kilometers zijn slechts enkele voorbeelden waarin toegang tot en (exclusief) beheer van gegevens hebben geleid tot de ontwikkeling van nieuwe en succesvolle commerciële verdienmodellen.

²⁹ Het onderzoek ziet bijvoorbeeld niet op gegevensuitwisseling zoals die wordt beoogd met het Wetsvoorstel Gegevensverwerking Samenwerkingsverbanden dat op dit moment in de Eerste Kamer wacht op behandeling.

De publieke sector heeft op bepaalde manieren ook geprofiteerd van deze ontwikkelingen, maar de reikwijdte van het ontwikkelen en inzetten van nieuwe technische methoden en toepassingen door de publieke sector is om diverse redenen beperkter gebleven. Die beperking is het gevolg van een aantal factoren. Zo kunnen actoren in de publieke sector enkel experimenteren en gebruik maken van nieuwe technologieën voor zover een formele wet hen dat toestaat of hen dat opdraagt. Private actoren kunnen daarentegen nieuwe technologieën ontwikkelen, inzetten en gebruiken tenzij de wet daaraan grenzen stelt. Dit uitgangspunt heeft bedrijven geholpen op zeer uiteenlopende terreinen te innoveren. Deze openheid van de wet voor activiteiten in de private sector heeft dezelfde sector in staat gesteld 'datagestuurde' markten aan te boren en te ontwikkelen. Succesvolle bedrijven bezitten en beheren tegenwoordig meer gegevens en zijn daarmee beter geïnformeerd dan overheden. Met name grote, globaal opererende bedrijven beheren en controleren veelgebruikte data-infrastructuren en de manier waarop gegevens aldaar worden beheerd. Daarmee kunnen deze bedrijven bepalen wie toegang tot hun gegevens krijgt, wie hun gegevens mag verwerken, en onder welke voorwaarden de gegevens worden gedeeld.

De dominantie van (grote) online platforms ten opzichte van (lokale) overheden is veelal terug te voeren op het feit dat digitale technologieën meestal zijn ontworpen en ontwikkeld door bedrijven, en veel minder door gemeenten of andere overheden. Dit heeft tot gevolg dat bedrijven de praktische, technische en epistemische voorwaarden bepalen ten aanzien van de wijze waarop gegevens toegankelijk zijn en worden beheerd, welke gegevens worden vastgelegd, opgeslagen, samengevoegd, geanalyseerd, overgedragen en gebruikt. Dit stelt deze bedrijven in staat exclusieve controle uit te oefenen over hoe die gegevens verwerkt en gebruikt kunnen worden. Deze exclusieve toegang en controle over het beheer van de gegevens vormt de kurk waarop veel bedrijfsmodellen van online platforms drijven.

De huidige ontwerpmethoden en -discussies rondom het beschikbaar maken van hebben zich tot nu toe ontwikkeld vanuit een 'engineeringperspectief' waarbij de vraag werd gesteld hoe het gebruik van nieuwe gegevensbronnen vanuit economisch perspectief met behulp van technische mechanismen verder kan worden gestimuleerd. Vanuit B2G-perspectief lijkt de discussie zich vooral te richten op de belangen van en voordelen voor bedrijven en gemeenten. Bij het definiëren van en onderhandelen over het beschikbaar maken van gegevens in B2G-relaties lopen burgers, met hun eigen rechten en belangen die gemoeid kunnen zijn met B2G het risico om slechts 'passieve' databronnen te worden. In een gemeente die haar beslissingen baseert op democratisch opgestelde regels in overeenstemming met de rechtsstaat, zouden burgers waar mogelijk eerder 'actieve' deelnemers moeten worden in een voorgenomen B2G.

2.2 Gemeentelijke overwegingen

Gemeentelijke toegang tot en gebruik van gegevens die in het bezit zijn van private organisaties, zoals online platforms, vervoersdiensten, websites over accommodaties, parkeergarages, supermarkten, energieleveranciers of financiële dienstverleners kan in sommige gevallen leiden tot betere analyses van maatschappelijke uitdagingen. Toegang tot en gebruikmaking van die gegevens via B2G biedt gemeenten mogelijkheden om te komen tot een meer accuraat en *evidence-based* beleidsvorming,

besluitvorming en uitvoering van publieke taken te verbeteren. Hieronder volgt een aantal overwegingen die een rol spelen bij het initiëren van B2G door de gemeente.

2.2.1 'Publieke taak'

De 'publieke taak' van een gemeente bepaalt over het algemeen in hoeverre B2G kan plaatsvinden in overeenstemming met het recht. Overheidsorganisaties kunnen in een rechtsstaat alleen handelen als de wet hen daartoe de bevoegdheid verleent of als de wet hen verplicht te handelen. Gemeenten zijn belast met een reeks taken. Zo moeten zij de volksgezondheid bevorderen, openbare ruimten onderhouden en beheren, rechtvaardige toewijzingen van sociale woningen garanderen, de afgifte van een beperkt aantal vergunningen in een bepaalde wijk op eerlijke wijze verdelen, rioleringen en afvalverwerking onderhouden, of openbaar vervoer of doorstroom van mobiliteit op gemeentelijk grondgebied faciliteren.

In het algemeen is het aan de rechtssystemen zelf om te bepalen wat een "publieke taak" inhoudt. De reikwijdte van de "publieke taak" is bekritiseerd omdat deze niet specifiek genoeg zou zijn. Voor de definitie van de "publieke taak" of van een "publiek belang" zijn de fundamentele rechten die zijn vastgelegd in de Grondwet en in het Europees Verdrag voor de Rechten van de Mens ('EVRM') richtinggevend. De Grondwet verplicht de overheid een recht op bijstand te realiseren, de bewoonbaarheid van het land en de bescherming van het leefmilieu te verbeteren, de volksgezondheid te bevorderen, en voldoende woongelegenheid te garanderen. Daarnaast zijn diverse publieke taken in gewone, specifieke of sectorale wetgeving vastgelegd.

Daarnaast kennen enkele wetten meer specifieke verplichtingen die bedrijven verplichten gegevens te delen met overheden, zoals het delen van gegevens ten behoeve van de berekening van de inkomstenbelasting, voor de informatiegaring door het Centraal Bureau voor de Statistiek (CBS), en onlangs trad de EU-Richtlijn in werking die online platformen verplicht informatie over verkopers die gebruikmaken van deze platformen, zoals hun inkomsten, door te geven aan de Belastingdienst met als doel transparantie in de digitale economie te vergroten. In deze gevallen ligt een publieke taak ten grondslag aan de verplichte gegevensdeling vanuit bedrijven die door de formele wetgever in een wet is vastgelegd.

2.2.2 Vrijwillige en verplichte B2G

B2G kan op zowel verplichte als op 'vrijwillige' basis plaatsvinden. Verplichte B2G is vastgelegd in de wet of te herleiden naar een wet. In de juridische literatuur zijn verschillende vrijwillige B2G-opties besproken: bedrijven kunnen zich bezighouden met B2G voor het algemeen belang door deel te nemen aan gegevenssamenwerkingsverbanden, ofwel sector-overstijgende samenwerkingsverbanden waarbij publieke of private actoren betrokken zijn bij het verzamelen, verwerken en uitwisselen van gegevens om een specifiek maatschappelijk probleem aan te pakken. Vrijwillige voorbeelden zijn te vinden in de transport-, nuts- en telecomsector. Bedrijven kunnen worden gestimuleerd om deel te nemen aan het delen van gegevens vanuit een 'altruïstisch' perspectief of om gegevens te doneren voor een humanitair doel dat is vastgelegd in publiek-private partnerschappen.

Naast verplichte en vrijwillige B2G in gemeentelijke context kan toegang tot en gebruik van bedrijfsgegevens soms een voorwaarde zijn voor acceptatie van een offerte in gemeentelijke aanbestedingsprocedures. Dit laatste betreft een vorm waarvan men zich kan afvragen of hier sprake kan zijn van vrijwillige B2G: een bedrijf kan immers niet offereën als het geen gegevens wil delen, terwijl er binnen de gemeente meestal geen redelijk alternatief is waar het wel kan offereën zonder B2G. Bij publiek-private overeenkomsten heeft de praktijk daarnaast uitgewezen dat B2G praktische problemen met zich kan meebrengen, zoals het ontbreken van een functionerende markt voor de prijsstelling van gegevens, wanneer gegevens bij bedrijven moeten worden aangekocht.

2.2.3 Juridische, technische en organisatorische mechanismen

Bij beleidsstukken rondom B2G gaat momenteel veel aandacht uit naar passende *technische* gegevensdeelmodellen die de gegevensverzameling en-uitwisseling mogelijk moeten maken. B2G bevat naast technische processen echter ook organisatorische en juridische mechanismen die noodzakelijk zijn om B2G te operationaliseren. Bij B2G moeten de juridische (in de vorm van wetgeving of contracten), organisatorische (in de vorm van afspraken over de verdeling van de taken en verantwoordelijkheden bij het tot stand brengen van B2G) en technische aspecten (waar gegevens die worden gebruikt voor B2G worden opgeslagen, op welke wijze de gegevens gereed worden gemaakt voor analyse, welke verwerking de meest accurate gegevens oplevert, of op welke wijze data transfers naar de gemeente plaatsvinden) op zodanige manier gereld zijn dat deze een samenhangende, consistente en rechtmatige B2G garanderen.

2.2.4 Burger- en maatschappelijk perspectief

In discussies over B2G ligt de nadruk veelal op de economische en commerciële rechten en belangen van bedrijven en op de bevoegdheden en beperkingen bij B2G aan de zijde van de gemeente. Bij het zoeken naar het juiste evenwicht tussen die rechten, belangen en noden en bevoegdheden rijst ook de vraag hoe de rechten en belangen van burgers die als gevolg van B2G kunnen worden geraakt, effectief worden beschermd. Het is immers de vraag of B2G altijd in overeenstemming is met rechten van burgers (zoals hun fundamentele rechten en hun rechten op bescherming van hun persoonsgegevens (zie hierna §3).

Gegevensbestanden die de gemeente ontvangt in het kader van B2G zullen in meer of mindere mate vooroordelen (biases) bevatten die kunnen leiden tot discriminatie wanneer deze bestanden worden ingezet ter uitvoering van beleid. Als deze risico's zich eenmaal in de (lokale) samenleving operationaliseren, kan het vertrouwen in de lokale overheid snel verdwijnen. Op gemeenten rust dan ook de verplichting dergelijke risico's uit te sluiten door bijvoorbeeld data protection impact assessments (DPIA)³⁰ of fundamental rights impact assessments (FRIA)³¹ te verrichten, of door

³⁰ Artikel 35 Algemene verordening Gegevensbescherming.

³¹ Zie J. Gerards, T. Schaefer, A. Vankan en I. Muis, Impact Assessment Mensenrechten en Algoritmes, Toolbox ethisch verantwoord innoveren van het Ministerie van Binnenlandse Zaken Koninkrijksrelaties <<https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes>> bezocht op 24 maart 2024; H. Janssen, M. Sengh-Ah Lee, J. Singh, Practical Fundamental Rights Impact Assessments (2022) International Journal of Law and Information Technology 20(2) 200

menselijke tussenkomst te organiseren op voorgenomen bewerkingen, al kleven aan dit type voorzorgsmaatregelen ook beperkingen.

Meer algemeen zal de vraag rijzen of B2G steeds het belang van 'de' burger dient: het is niet altijd duidelijk of met B2G het dienen van belangen van *alle* burgers worden beoogd, of dat de belangen van enkele burgers worden gediend en hoe zich het gebruik van de gegevens verhoudt tot het recht op gelijke behandeling van burgers. Het kan lastig zijn te definiëren wie meer precies 'de' burger is. Burgers zijn immers verschillend als het aankomt op bijvoorbeeld kansen op de arbeidsmarkt, de woningmarkt, afstand tot gezondheidsvoorzieningen of digitale geletterdheid.

2.3 Overwegingen van bedrijven

Tijdens interviews gaven sommige bedrijfsmedewerkers aan dat binnen bedrijven bereidheid kan bestaan gegevens met de gemeente te delen omwille van publieke doelstellingen, zoals het oplossen van verkeerscongestie of het bewaken van de fysieke veiligheid van burgers in openbare of publiek toegankelijke ruimten. Ook bestaan bij bedrijven zorgen over B2G gegevensdeling; deze zijn gedocumenteerd in literatuur en werden ook benoemd tijdens interviews met bedrijfsmedewerkers.

2.3.1 Zorgen

Hieronder worden overwegingen van bedrijven weergegeven die een rol kunnen spelen bij de terughoudendheid gegevens te delen voor publieke doeleinden. Deels werden deze geuit door medewerkers, deels zijn ze expliciet in de literatuur geuit. Bedrijfsmedewerkers uitten hun zorgen over:

- de naleving van de AVG door het bedrijf: zij zijn onzeker over de verplichtingen voor gegevensbeheerder, aansprakelijkheidskwesties, reputatierisico's wanneer persoonsgegevens worden gedeeld in B2G;
- niet-naleving van bescherming van intellectuele eigendomsrechten;
- niet-naleving van bescherming van bedrijfsgeheimen en gerelateerde aansprakelijkheidskwesties die met B2G gepaard kunnen gaan als de gemeente;
- overheidsinstanties die bedrijfsgegevens mogelijk niet in overeenstemming met bredere, toekomstgerichte bedrijfsbelangen behandelen;
- een beweerdelijk gebrek aan een 'gegevensuitwisselingscultuur' in overheidsorganisaties, d.w.z. afwezigheid van kennis over hoe publieke waarde kan worden gecreëerd, beperkte middelen capaciteit, gebrek aan vaardigheden en beperkt vertrouwen van burgers, wat reputatierisico's met zich mee kan brengen;
- tegenstrijdige belangen; in sommige sectoren (bv. mobiliteit) kunnen bedrijven alleen aan B2G doen als een kritische massa van concurrenten hetzelfde zal doen; B2G kan immers leiden tot situaties waarin sommige bedrijven geen prikkel (meer) hebben om te delen omdat anderen dat al doen, en dat degenen die meedoen potentieel marktaandeel kunnen verliezen;
- kosten die het bedrijf moet maken vanwege investeringen in nieuwe technologieën of processen om aan B2G te kunnen voldoen;
- gegevenskwaliteit met betrekking tot nauwkeurigheid en volledigheid van gegevens, en angst dat deze verkeerd kunnen worden geïnterpreteerd of gebruikt;

- dat bedrijven gegevens en gegevensbestanden als hun belangrijkste activa beschouwen; B2G nu of in de toekomst kan leiden tot afwaardering van hun activa waardoor het bedrijf concurrentieslagkracht kan verliezen;
- dat gegevens worden gebruikt en verder gedeeld voor doeleinden die niet overeenkomen met hun eigen belangen;
- dat bedrijven geen direct voordeel zien in B2G en daardoor minder bereid zijn gegevens te delen, al is dit anders wanneer dit wordt vereist door wet- of regelgeving;
- politiek (deels) onvoorspelbare factoren, zoals veranderingen in het beleid van overheden of regelgevende instanties, de mogelijke impact van deze veranderingen op hun bedrijfsvoering en voor de vertrouwelijkheid van hun gegevens.

2.3.2 Kansen

In literatuur, verslagen van relevante workshops en gesprekken met medewerkers komt ook naar voren dat B2G ook mogelijkheden en kansen kan opleveren voor bedrijven. Door deel te nemen aan B2G kan een bedrijf kennis opbouwen over de informatie die de gemeente nodig heeft bij het krijgen van meer zichtbaarheid op behoeften van gemeenten. B2G kan een bedrijf mogelijkheden bieden een goede reputatie op te bouwen binnen een gemeente, hetgeen nieuwe zakelijke perspectieven kan openen, waarbij de gemeente zou kunnen overwegen dat bedrijf een bevoorrechte positie te geven ten opzichte van andere bedrijven die zij niet kent (al dient een gemeente zich ook te houden aan wettelijke verplichtingen zoals gelijke behandeling). Ook bestaan voorbeelden van altruïstisch georiënteerde B2G waarbij bedrijven gegevens beschikbaar stellen aan openbare dienstverleners met het oog op maatschappelijk verantwoord ondernemen, hetgeen reputatievoordelen kan bieden. B2G in het kader van gemeentelijke vergunningverlening kan een bedrijf ook voordelen brengen, bijvoorbeeld wanneer een vergunning, een middel om schaarse goederen (zoals openbare ruimte) te verdelen, ertoe leidt dat een beperkt aantal bedrijven gebruik mag maken van dat goed.

2.4 Voorgestelde strategieën voor ontsluiting van gegevens

Gelet op de potentiële juridische risico's en kosten voor bedrijven en de juridische, sociaal-politieke en technische uitdagingen voor gemeenten worden soms ook alternatieve methoden voor B2G overwogen, met name wanneer (fundamentele) rechten en belangen van bedrijven, burgers en consumenten in het geding kunnen zijn. Hierna volgen enkele benaderingen en voorbeelden waarmee juridische risico's tot op zekere hoogte zouden kunnen worden weggenomen. Ze werden genoemd in interviews en in enkele externe expertsessies. De benaderingen zijn situatie-gebonden; sommige strategieën zijn beter in een bepaalde situatie toe te passen dan andere.

2.4.1 Privacy Enhancing Technologies

Voor bedrijven die toegang verlenen tot gevoelige informatie waarover zij beschikken, zoals gegevens met betrekking tot natuurlijke personen, intellectuele eigendomsrechten of bedrijfsgeheimen, is het belangrijk om een balans te vinden tussen risico's, kosten en controle over de toegang in B2G. Specifieke technische en organisatorische maatregelen worden vaker samengepakt in de term *Privacy*

Enhancing Technologies (PETs). PETs kunnen soms helpen bij de afscherming van gegevens waardoor ze niet of zeer beperkt zichtbaar zijn en daarmee een veiliger en beter beveiligde gegevensuitwisseling en-toegang beloven. Enkele typische maatregelen zijn *multi-party computation*, *homomorfic encryption*, *zeroknowledge proofs*, anonimisering van gegevens, *differential privacy*, *federated learning*, *trusted execution environments* en het gebruik van *synthetische gegevens*.³²

Afhankelijk van de aard, de reikwijdte, de context en de doeleinden van de toegang tot en het gebruik van gegevens, zijn PETs niet overal inzetbaar. Elke technologie die tot doel heeft de persoonlijke levenssfeer van de betrokkenen bij een gegevensuitwisseling te bevorderen, heeft zijn eigen sterke punten, beperkingen, kosten en expertisevereisten. Uit recent onderzoek blijkt dat hoewel de technische verfijning van PETs voortschrijdt, het gebruik ervan relatief laag blijft omdat het veel organisaties ontbreekt aan deskundigheid. Organisaties zijn daardoor mogelijk niet goed in staat de kansen en de risico's van het gebruik van een bepaalde PET in te schatten.

In de context van B2G kunnen kennis over de doeltreffendheid, beperkingen en mogelijkheden van PETs van groot belang zijn omdat deze de vertrouwelijkheid van de gegevensdeling mogelijk verder kunnen verbeteren. Dit moet verder worden onderzocht.

2.4.2 Differentiatie in het type informatie dat wordt gedeeld

Het delen van informatie met de gemeente kan op verschillende detailniveaus plaatsvinden. In de literatuur worden doorgaans vier detailniveaus van gegevensdeling aangenomen:

- (i) gegevens die worden gedeeld kunnen onbewerkt zijn (zoals ze bij de bron zijn verzameld);
- (ii) gegevens kunnen voorbewerkt zijn (bijv. opgeschoond en voorbereid voor berekeningen en analyses);
- (iii) gegevens kunnen bewerkt zijn (berekend, samengevoegd en gecombineerd); of
- (iv) gegevens die samengevoegd zijn in data-gestuurde inzichten die het resultaat zijn van berekeningen, analyses en samenvoegingen.³³

Bedrijven hebben een sterke voorkeur voor het delen van gegevens op het hoogste aggregatieniveau zoals wanneer informatie wordt gedeeld die is gebaseerd op gestuurde inzichten onder (iv). Zij delen liever geen bestanden met ruwe gegevens. Het delen van inzichten stelt hen in staat beter controle te houden over de gegevens. Tegelijkertijd kunnen de juridische en economische risico's worden beperkt. Hoewel deze aanpak veelbelovend lijkt, moeten voor elke specifieke B2G de risico's alsnog worden geïdentificeerd en beoordeeld, aangezien het delen van resultaten bijvoorbeeld nog steeds verwijzingen naar of onthulling van persoonsgegevens of bedrijfsgeheimen kan bevatten wanneer de ontvangen gegevensbestanden worden samengevoegd met andere gegevensbestanden, of omdat een

³² Zie voor en uitleg van PETs bijvoorbeeld The Royal Society, *From Privacy to Partnership. The role of privacy enhancing technologies in data governance and collaborative analysis* (London, januari 2023). 20232023)(Janu2023)<https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/from-privacy-to-partnership.pdf>.

³³ M. Micheli, *Public bodies' access to private sector data: The perspectives of twelve European local administrations*, First Monday (februari 2022) <https://doi.org/10.5210/fm.v27i2.11720>.

ontvangen bestand veelal vooroordelen (biases) bevat die zich kan vertalen in discriminerende toepassingen.

2.4.3 Aanvullende strategieën

Het belang van het definiëren van gedeelde doelstellingen

Een van de geïnterviewden bracht een *use case* naar voren waarin werd gesproken over gemeenten die beperkingen van de verhuur van particuliere woningen door leden van Airbnb effectief wilden kunnen handhaven op basis van lokale wetgeving. Airbnb wilde geen gegevens over verhuur delen; het bedrijf beriep zich op de privacyrisico's van huiseigenaren en bezoekers, en antwoordde dat het bovendien geen real-time gegevens over personen die hun woning verhuren kon delen omdat dit de positie van Airbnb op de beurs zou kunnen beïnvloeden.

Een onafhankelijke derde (een tussenpersoon) werd geïntroduceerd om te verkennen of Airbnb op een andere wijze kon helpen bij de naleving van de verhuurgrens. De wettelijke verplichting bleek op dat moment niet voldoende handvatten te hebben om deze te handhaven. De oplossing die Airbnb, de tussenpersoon en de gemeente uiteindelijk overeenkwamen was niet om locatiegegevens of exacte en real-time aantallen verhuurde dagen te delen, maar dat Airbnb, dat immers zelf informatie heeft over het aantal verhuurdagen en op de hoogte is van het maximum aantal verhuurdagen dat de gemeente toelaat, zelf de huiseigenaar in kwestie zou informeren over het naderen van het maximum aantal verhuurdagen door een specifieke verhuurder, en daarmee langs deze weg zou meewerken aan de naleving van de wet. Om Airbnb te overtuigen van het belang van het delen van geaggregeerde informatie, definieerden de tussenpersoon, de gemeente en Airbnb een gezamenlijk doel: zowel de gemeente als Airbnb hebben belang bij het leefbaar en aantrekkelijk houden van steden voor zowel de inwoners als de bezoekers.

Vraag gegevens op een detailniveau dat aansluit op de aanpak van het specifieke probleem

Voordat een passende B2G tot stand kan worden gebracht, dient duidelijk te zijn voor welk doel de gegevens precies worden opgevraagd en welk type informatie daarvoor precies nodig is. Dit vereist goede kennis bij de partij die gegevens wenst te ontvangen over het bezit van de eigen gegevens en over het probleem dat opgelost moet worden. Een probleem laat zich vaak niet oplossen met een ongesorteerde set data; bijna altijd is maatwerk noodzakelijk. Zo wilde een gemeente bijvoorbeeld automobilisten op drukke dagen informeren over beschikbare parkeerplaatsen in en om de stad op basis van real-time informatie, maar parkeerbedrijven wilden geen gegevens delen omdat die gegevens deel uitmaken van hun bedrijfsgeheim en het delen van gegevens concurrentiegevoeligheden met zich mee kan brengen.

Een onafhankelijke derde (ook een tussenpersoon) slaagde er echter in gegevens met een lage gevoeligheid te verkrijgen door informatie op te vragen om bestuurders voldoende nauwkeurig te informeren zodat zij een beter geïnformeerde keuze zouden maken voor een parkeerplaats in plaats van naar de dichtstbijzijnde parkeerplaats te rijden die al volledig bezet bleek. Bij parkeren blijkt dat als minder dan 60% van de plaatsen in een garage bezet is, bedrijfsinformatie niet interessant is. Vanaf > 90% bezetting wordt de bezettingsgraad van de garage wel relevant. Zo bleek dat de gemeente, om haar publieke taak – mobiliteitsbeheer in de openbare ruimte – geen heel precieze gegevens nodig

heeft. In plaats daarvan is een indicatie van >90% (zonder specifieker te worden) en van de snelheid waarmee parkeerplaatsen vol raken, voldoende nauwkeurig om bestuurders accuraat te informeren. Dit betreft in het kader van differentiatie het type (iv) data dat gedeeld wordt (§2.4.2)

Aangezien de waarde van zulke meer abstracte informatie over het algemeen lager is, worden de potentiële risico's voor bedrijfsgeheimen lager, terwijl de gemeentelijke doelstelling alsnog kan worden bereikt. Deze strategie slaagde erin de bedrijfsrisico's te verlagen zonder de nauwkeurigheid te verliezen die nodig is om bestuurders te informeren.

Identificeer en beoordeel het exacte probleem dat moet worden opgelost

Dit werd hiervoor al even aangestipt. Het lijkt een voor de hand liggende suggestie als het gaat om gegevenstoegang en-deling, maar vaak blijkt het nog niet zo gemakkelijk om het precieze doel bij het gegevensverzoek te formuleren. De formulering van het doel bepaalt in hoge mate welke gegevens nodig zijn om het probleem te adresseren. Dat blijkt uit het volgende voorbeeld: een gemeente wil inwoners informeren die in aanmerking komen voor een eenmalige uitkering voor energie (energietoeslag). Het blijkt voor de gemeente in de praktijk echter erg lastig om te bepalen wie voor die toeslag in aanmerking komt omdat degenen die er recht op lijken te hebben, niet uit zichzelf naar de gemeente stappen. De gemeente overweegt vervolgens een lokaal opererend energiebedrijf te vragen om gegevens van inwoners die hun energierekeningen drie maanden op een rij niet konden betalen, zodat de gemeente hen kan informeren over het feit of ze in aanmerking komen voor het energievoordeel.

Hier zou de gemeente het ook anders kunnen aanpakken. Zij zou het precieze probleem moeten identificeren, en op basis daarvan het specifieke doel van gegevensuitwisseling moeten bepalen om te beoordelen of en welke gegevens de gemeente van het energiebedrijf nodig zou hebben om het probleem op te lossen. Het gaat in dit geval *niet* om het voorkomen dat mensen in een schuldental terecht zouden komen door torenhoge energieprijzen, maar om te voorkomen dat mensen in de winter afgesloten zouden worden van elektriciteit en gas door ze toeslagen te geven waar ze recht op hebben. Deze aanpak toont enige gelijkenis met de situatie met Airbnb.

Om redenen van gegevensminimalisatie mag een gemeente alleen gegevens opvragen die nodig zijn om een specifiek geïdentificeerd probleem op te lossen. Het is steeds belangrijk om dat specifieke doel voor het delen van gegevens zo precies mogelijk te definiëren. De gemeente zou met het doel het voorkomen dat mensen in de winter afgesloten worden van gas en elektra, kunnen overwegen om het bedrijf, dat zicht heeft op de betalingen van inwoners, te vragen om mensen op de hoogte te stellen van hun recht op die toeslag. In dat geval is het niet nodig dat gegevens met de gemeente worden gedeeld.

3. Wettelijk kader bij B2G

Rondom B2G door bedrijven met overheden en meer specifiek met gemeenten is een palet van Europese en nationale wet- en regelgeving van toepassing. Een recente analyse van het Nederlands

juridisch kader dat van toepassing is op gegevensdeling door bedrijven met een gemeente leverde het volgende beeld op.³⁴

3.1 Fundamentele rechten

Een door een gemeente geïnitieerde B2G – verplicht of vrijwillig – kan raken aan de fundamentele rechten van burgers en van bedrijven. Deze rechten zijn neergelegd in de Grondwet, het Europees Verdrag voor de Rechten van de Mens, het EU-Handvest van de Grondrechten en in internationale documenten. Deze rechten beschermen burgers tegen overheidsoptreden dat ingrijpt op deze rechten. Fundamentele rechten zijn echter niet absoluut. Een overheid kan de werking van de rechten beperken onder de voorwaarden dat een dergelijke beperking in een formele wet is neergelegd; dat een dergelijke beperking een welomschreven doel dient, en dat de beperking noodzakelijk is in het belang van een democratische samenleving.

Gegevens verkregen uit B2G kunnen een bias bevatten, waardoor het gebruik van die gegevens door de gemeente voor analysedoeleinden om daar beleid op af te stemmen kan leiden tot beperkingen op het grondwettelijk discriminatieverbod. Ook de rechten op privacy en de bescherming van persoonsgegevens kunnen onder druk komen te staan, bijvoorbeeld wanneer de door de gemeente ontvangen gegevensbestanden naar personen herleidbare gegevens bevatten. De gemeente mag die gegevens niet ontvangen en gebruiken, tenzij haar voor het gebruik van de gegevens een bevoegdheid bij wet is toegekend.

Fundamentele rechten richten zich niet alleen op burgers, zij kennen ook bescherming toe aan bedrijven, zoals het recht van bedrijven om informatie te ontvangen en te verstrekken, de vrijheid van ondernemerschap zoals vastgelegd in art. 16 van het EU-Handvest voor de Grondrechten, of (intellectuele) eigendomsrechten.

B2G die raakt aan fundamentele rechten is daarmee niet verboden, maar de wetgeving stelt wel voorwaarden aan B2G die deze rechten raakt.

3.2 Algemene verordening gegevensbescherming

Wanneer in B2G-context persoonsgegevens worden verwerkt (gegevens die te herleiden zijn naar een geïdentificeerd of identificeerbare persoon, de ‘betrokkene’),³⁵ is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De term ‘verwerken’ moet breed worden opgevat; hieronder vallen ook anonimiseren, pseudonimiseren, opvragen, raadplegen, afschermen, wissen of vernietigen.³⁶ De AVG heeft primair tot doel persoonsgegevens te beschermen omdat de verwerking van deze gegevens in dienst van betrokkenen moet staan en deze niet alleen ten goede moet komen aan overheden of bedrijven. Daarnaast heeft de AVG tot doel de positie van de betrokkenen ten opzichte van degenen die hun gegevens verwerken te versterken. De AVG biedt betrokkenen hiertoe

³⁴ Janssen, Verboeket en Meiring (2023).

³⁵ Art. 4(1) AVG.

³⁶ Art. 4(2) AVG.

een reeks informatie- en inzagerechten waaraan verwerkingsverantwoordelijken (degenen die het doel van de verwerking bepalen) moeten voldoen.³⁷ De gemeente treedt in te context van B2G op als verwerkingsverantwoordelijke voor zover zij in B2G bepaalt voor welk doel de gegevens die in het bezit zijn van een bedrijf moeten worden verwerkt.³⁸ Zij treedt ook op als verwerkingsverantwoordelijke voor zover zij een bedrijf de opdracht geeft tot het anonimiseren van een gegevensbestand dat het wordt geacht te delen met de gemeente.

Artikel 5, eerste lid, AVG bevat de kernbeginselen van het gegevensbeschermingsrecht. De verwerkingsverantwoordelijke is verplicht de persoonsgegevens op een wijze te verwerken die voor de betrokkene rechtmatig, behoorlijk en transparant is (a), terwijl de gegevens die worden verwerkt alleen mogen worden gebruikt voor het doel waarmee ze oorspronkelijk zijn verkregen (b). Artikel 5 AVG schrijft verder voor dat alleen de gegevens worden verzameld en verwerkt die toereikend zijn voor de doeleinden waarvoor zij worden verwerkt (c), dat de gegevens juist dienen te zijn en zo nodig moeten worden geactualiseerd (d). Ook worden er eisen gesteld aan de wijze waarop de gegevens opgeslagen worden (e) en eisen gesteld met betrekking tot integriteit en vertrouwelijkheid (onderdeel f).

In B2G kan onder meer het doelbindingsbeginsel onder druk komen te staan omdat persoonsgegevens die bedrijven verwierven voor hun eigen doel vervolgens door de gemeente voor een ander doel worden gebruikt. Het doelbindingsbeginsel vereist dat persoonsgegevens niet gebruikt mogen worden voor een ander doel dan het doel waarvoor ze oorspronkelijk zijn verkregen. De AVG laat secundair gebruik echter toe wanneer het doel waarvoor de gegevens gebruikt worden, verenigbaar is met het doel waarmee ze oorspronkelijk werden verkregen. In essentie rust het doelbindingsbeginsel op twee fundamenten. Om te kunnen beoordelen in hoeverre het doelbindingsbeginsel het verdere gebruik toelaat, is allereerst vereist dat de secundaire doelstelling waar de gegevens voor gebruikt worden voldoende concreet is beschreven. Gegevensverwerking in B2G kan alleen rechtmatig plaatsvinden voor ‘specified, explicit and legitimate purposes’, ofwel specifiek omschreven en helder geformuleerde doeleinden die passen binnen een wettelijke doelstelling uit de AVG.³⁹ Het tweede fundament betreft de (on)verenigbaarheid van het gebruik van gegevens voor een doel, die oorspronkelijk voor een ander doel werden verzameld.⁴⁰ In de beoordeling van de verenigbaarheid dient de verwerkingsverantwoordelijke na te gaan (i) ieder verband tussen de doeleinden waarvoor de persoonsgegevens werden verzameld en de doeleinden van de voorgenomen secundaire verwerking; (ii) de context waarbinnen de gegevens zijn verzameld en de mate waarin de betrokkene kan verwachten dat diens gegevens voor een ander doel worden gebruikt; (iii) de aard van de gegevens en de eventuele gevoeligheid daarvan; (iv); de mogelijke gevolgen van de voorgenomen secundaire verwerking voor de betrokkene; en (v) de maatregelen die de verwerkingsverantwoordelijke treft ter bescherming van de persoonsgegevens.⁴¹ Beide hoekstenen vereisen helder omkaderde doelstellingen waarbinnen gegevensverwerking rechtmatig mogelijk is: het doelbindingsbeginsel is sterk verbonden

³⁷ Artt. 13 en 14 (ex ante informatierechten) en jo. 15 tot en met 22 (ex post informatierechten) Avg.

³⁸ Art. 4(7) AVG; Article 29 Working Party Opinion 1/2010 on the concepts of “controller” and “processor” adopted on 16 February 2010, 264/10/EN, WP 169; EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (aangenomen op 2 September 2020).

³⁹ Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203.

⁴⁰ Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203.

⁴¹ Art. 6(4) (a)-(d) AVG.

met de beginselen van transparantie en daardoor ook het beginsel van voorzienbaarheid.⁴² Transparantie over de doelen waarvoor de (verwerkte) gegevens gebruikt kunnen worden biedt bovendien de betrokkene inzicht in de verwerkingen.

Verwerkingsverantwoordelijken kunnen persoonsgegevens alleen verwerken op basis van één van de in de AVG genoemde rechtsgronden.⁴³ Met het oog op B2G zijn onderdelen (c) 'de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust' en (e) 'de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag [...]' het meest voor de hand liggend. Wanneer B2G wordt voorgeschreven op basis van één van deze AVG-grondslagen, dienen deze terug te voeren zijn op een specifieke wet in formele zin. De betreffende wetgeving moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde, gerechtvaardigde doel.⁴⁴ De rechtsgrond moet voldoende duidelijk en nauwkeurig zijn zodat de toepassing ervan voorspelbaar of voorzienbaar is voor degenen op wie deze van toepassing is.⁴⁵

Een gemeente kan wanneer sprake is van een situatie waarin een bedrijf vrijwillig gegevens deelt, een dergelijke deling baseren op een contract. In gegevensbestanden die in vrijwillige context met een gemeente worden gedeeld mogen echter geen persoonsgegevens aanwezig zijn; verwerking ervan door de gemeente dient immers op een wettelijke grondslag te berusten.

Verwerkingsverantwoordelijken moeten passende technische en organisatorische maatregelen nemen om te waarborgen en aan te kunnen tonen dat hun verwerking in overeenstemming met de AVG wordt uitgevoerd.⁴⁶ Daarnaast moet de verwerkingsverantwoordelijke de hiervoor genoemde informatie- en inzage-rechten van betrokkenen naleven.

3.3 AI-Verordening

De AI-verordening is van toepassing op aanbieders en gebruikers – waaronder ook bedrijven en overheden – van AI-systemen. Op hen rust een reeks verantwoordelijkheden en verplichtingen; bedrijven en overheden die AI-systemen willen gebruiken, zullen voorafgaand aan de inzet van een AI-systeem moeten beoordelen of het systeem een 'onaanvaardbaar', 'hoog' of 'laag' risico met zich meebrengt voor de gezondheid, de veiligheid en de fundamentele rechten van personen. Afhankelijk van de risicokwalificatie gelden specifieke regels. AI-systemen uitgerust met software voor biometrische identificatie op afstand – zowel real-time als achteraf – gelden bijvoorbeeld als AI-systemen met een hoog risico. Gebruikers van die hoog-risicosystemen zijn verplicht om voorafgaand aan het gebruik van hoog-risico-systemen een fundamental rights impact assessment te verrichten.

Voor publieke actoren kent de AI-Verordening geen zelfstandig regime rondom het gebruik van AI-systemen. De Verordening verbiedt het gebruik van AI-systemen die de betrouwbaarheid van

⁴² Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203.

⁴³ Art. 6(1) AVG.

⁴⁴ Art. 6(3) AVG.

⁴⁵ Overweging 41 AVG.

⁴⁶ Art. 5(2) AVG.

natuurlijke personen op basis van hun gedrag analyseren ('social scoring'). De overige bepalingen in de Verordening die het gebruik in de publieke sector reguleren, zien op toepassingen ten aanzien van rechtshandhaving, en vallen daarmee buiten het bestek van dit onderzoek. De AI-Verordening lijkt het gebruik van biometrische identificatie op afstand wel toe te staan voor niet-wetshandavingsdoeleinden, zoals *crowd control* of volksgezondheid.⁴⁷ Zulke toepassingen vallen, voor zover persoonsgegevens worden verwerkt eveneens onder het bereik van de AVG, en voor zover deze verwerkingen burgers raken ook onder de Grondwet, het EU-Handvest en het EVRM.

3.4 Wet bescherming bedrijfsgeheimen

Gegevens in B2G kunnen betrekking hebben op vertrouwelijke bedrijfsinformatie die wordt beschermd door de Wet bescherming bedrijfsgeheimen. Deze wet beschermt een houder van bedrijfsgeheimen tegen onrechtmatige verkrijging door derden, en tegen het gebruik of de openbaarmaking van het bedrijfsgeheim wanneer dit gebeurt zonder toestemming van de houder van het bedrijfsgeheim. Bedrijfsgeheimen beperken daarmee de mate waarin een gemeente de gegevens die zij verkreeg via B2G verder kan delen met derden (bijvoorbeeld ten behoeve van innovatiedoelstellingen).

Openbaarmaking en verder delen van gegevens die via B2G zijn verkregen, zijn onderworpen aan beperkingen die worden opgelegd door de Wet open overheid (zie hierna §3.5) die een gemeente dan in overweging moet nemen. Naast de bescherming van bedrijfsgeheimen kunnen in B2G intellectuele eigendomsrechten zoals (met name) het databankenrecht en mogelijk het auteursrecht van bedrijven betrokken raken.

3.5 Wet open overheid

De Wet open overheid (Woo) regelt de voorwaarden waaronder actoren in de publieke sector informatie openbaar moeten maken, alsook de voorwaarden die publieke actoren kunnen verbinden aan het openbaar maken van gegevens. Wanneer de gemeente via B2G bedrijfsgegevens ontvangt die raken aan de publieke taak van de gemeente, kan de Woo ertoe leiden dat de gemeente deze gegevens (deels) openbaar moet maken. Algemeen geldt echter dat een gemeente gegevens die zijn verkregen via B2G openbaar moet maken, behalve als de rechten en redelijke belangen zoals de bescherming van persoonsgegevens, bedrijfsgeheimen en intellectuele eigendomsrechten zich hiertegen verzetten. Op deze uitzonderingen bestaan echter weer uitzonderingen, bijvoorbeeld als een zwaarwegend algemeen belang, zoals het belang van de openbare veiligheid, de volksgezondheid, het milieu of de bescherming van de democratische rechtsorde, dit in een specifiek geval vereist.

3.6 Open Data Richtlijn en Wet Hergebruik Overheidsinformatie

De EU-Richtlijn Open Data moedigt overheidsinstanties aan informatie actief beschikbaar te stellen voor hergebruik met zo min mogelijk voorwaarden die dat hergebruik beperken. De EU-Richtlijn regelt

⁴⁷ M. Veale & F. Zuiderveen Borgesius, 'Demystifying the draft EU Artificial Intelligence Act' (2021) *Computer Law Review International* 4, p. 97.

niet de toegang tot overheidsinformatie. In situaties waarin de gemeente via B2G gegevens verkreeg van bedrijven, en deze niet worden beschermd zoals bepaald onder de Wet open overheid (zie §3.5), kan iedereen verzoeken om hergebruik van de gegevens voor commerciële of niet-commerciële doeleinden. Overheidsinstanties mogen voorwaarden stellen aan hergebruik, maar dat kan alleen als die voorwaarden noodzakelijk, transparant en niet-discriminerend zijn. Gelijke groepen afnemers moeten met andere woorden gelijk worden behandeld om een gelijk speelveld te garanderen.

3.7 Algemene wet bestuursrecht⁴⁸

Overheden hebben vanwege hun taakvervulling in het kader van de behartiging van het algemene, publieke belang vergaande, exclusieve bevoegdheden. Overheden nemen vanwege deze taken en verantwoordelijkheden in het maatschappelijke verkeer een bijzondere plaats in. Tegenover deze bevoegdheden staat dat overheden algemeen aan strengere normen gebonden zijn dan bedrijven en particulieren. Dat geldt ook bij het verkrijgen van gegevens die in bezit zijn van bedrijven. Het grondrechtelijk kader (§3.1) en de AVG (§3.2) zijn als het gaat om toelaatbare gegevensverwerking door de overheid in B2G-context erg belangrijk.

Gemeenten hebben diverse bestuursrechtelijke instrumenten in te zetten waar het gaat om het verkrijgen van toegang tot gegevens die in bezit zijn van bedrijven. Hiertoe behoren publiekrechtelijke instrumenten, zoals het afkondigen van een gemeentelijke verordening, het opstellen van een vergunningstelsel en een daarop gebaseerde vergunningverlening of een subsidie, en privaatrechtelijke instrumenten, zoals overeenkomsten, overheidsopdrachten of concessies.

De instrumentkeuze is niet vrij. Aan de keuze voor een instrument zijn voorwaarden verbonden die te vinden zijn in de Algemene wet bestuursrecht (Awb) en in de algemene beginselen van behoorlijk bestuur (abbb) en de bijbehorende rechtspraak. De bevoegdheid van de gemeente om een publiekrechtelijk instrument in te zetten voor B2G is publiekrechtelijk geregeld, zoals (Europese) verordeningen, grondrechten en algemene beginselen van behoorlijk bestuur. Overweegt de gemeente een privaatrechtelijk instrument in te zetten, dan vloeit de bevoegdheid daartoe voort uit het privaatrecht.

Het gebruik van de bestuursrechtelijke instrumenten wordt algemeen beperkt door de verplichtingen van de gemeente op grond van de Grondwet, de Awb, en de abbb.⁴⁹ Daarnaast is een belangrijk uitgangspunt voor de inzet van privaatrechtelijke instrumenten dat de gemeente niet kan 'ontsnappen' aan wettelijke voorschriften door gebruik te maken van haar privaatrechtelijke bevoegdheden, en dat publiekrechtelijke regelingen die publiekrechtelijke bevoegdheden van de gemeente reguleren, altijd voorgaan.

De inzet van vrijwel alle bestuurlijke instrumenten vereist proportionaliteit bij het opleggen van de eisen die worden gesteld aan bedrijven teneinde B2G tot stand te brengen. Ook is een duidelijk en nauw verband vereist tussen de opgelegde eisen en het achterliggend doel van de inzet van het

⁴⁸ Zie voor uitgebreide analyse van de relevante Awb-aspecten Janssen, Verboeket en Meiring (2023), § 3.3.

⁴⁹ M.W. Scheltema, 'Doorwerking van het publiekrecht in het privaatrecht in drievoud', [BJU 2009](#).

betreffende instrument.⁵⁰ Het opleggen van eisen vanuit de gemeente moet aldus op weloverwogen wijze gebeuren, al zijn de precieze begrenzings van situaties waarin dat verband wel of niet meer bestaat niet helder.⁵¹

3.8 Data Verordening

Onlangs nam EU-wetgever de Data Verordening aan. Hoofdstuk V van de Data Verordening beoogt de rechten en verplichtingen van (overwegend) bedrijven in B2G te reguleren en de bevoegdheden van overheden te normeren. De Verordening is van toepassing op alle maatschappelijke sectoren. Deze reguleert enkel verplichte B2G, en niet de vrijwillige B2G. De Verordening beperkt de toelaatbaarheid van B2G op twee manieren.

Allereerst kan een overheidsinstantie alleen toegang krijgen tot gegevens en deze gebruiken wanneer dit noodzakelijk is om te reageren op een noodsituatie, of wanneer de gegevens nodig zijn om een dergelijke noodsituatie te voorkomen en de overheidsinstantie niet in staat is om deze gegevens tijdig en effectief via alternatieve wegen te verkrijgen. In die gevallen moet sprake zijn van een door de overheid aan te tonen (dreiging van een) noodsituatie. Het merendeel van de verzoeken om B2G zal waarschijnlijk niet zo snel in deze categorie van gevallen voorkomen, omdat de in de wet omschreven noodsituaties zich niet vaak voordoen en omdat het aantonen van dreigende noodsituaties voor overheden erg lastig kan zijn.

B2G zal eerder voorkomen in de tweede categorie van gevallen, die buiten de acute en dreigende noodsituaties, bijvoorbeeld wanneer een overheidsinstantie door een gebrek aan gegevens een haar bij wet toegewezen taak algemeen belang niet kan vervullen. In die gevallen bepaalt de Data Verordening dat die overheidsinstantie toegang kan eisen onder de volgende voorwaarden:

- (i) in verplichte B2G kan het enkel gaan om gegevens die niet ook persoonsgegevens zijn;
- (ii) de overheid handelt op basis van een wet en heeft specifieke gegevens geïdentificeerd waartoe zij toegang zou willen; het ontbreken van die gegevens hindert haar echter bij het vervullen van de door de wet opgelegde, specifieke taak (zoals de productie van officiële statistieken of de beperking van of het herstel na een noodsituatie), *en*
- (iii) de overheid heeft alle andere middelen waarover zij beschikt om deze gegevens te verkrijgen uitgeput, inclusief de aankoop van gegevens op de markt tegen markttarieven, of door een beroep te doen op bestaande verplichtingen om gegevens beschikbaar te stellen, of wanneer de goedkeuring van nieuwe wetgevende maatregelen de tijdige beschikbaarheid van de gegevens niet kan garanderen.
- (iv) Kleine ondernemingen vrijgesteld van de verplichting om gegevens te delen buiten situaties van (dreigende) noodsituaties.

De Verordening laat ruimte voor de formele wetgever voor het reguleren van verplichte B2G-gegevensdeling. Een enkel voorbeeld is te vinden in de specifieke regeling van artikel 30c Wet personenvervoer 2000; deze bepaling verleent de minister van Infrastructuur en Milieu de bevoegdheid regels te stellen over het verplicht beschikbaar stellen, door concessiehouders, van

⁵⁰ Janssen, Verboeket en Meiring. (2023), § 3.3.

⁵¹ Janssen, Verboeket en Meiring. (2023), § 3.3.

geanonimiseerde gegevens over reizigersstromen die uit het gebruik van vervoerbewijzen zijn af te leiden. De minister heeft van deze bevoegdheid tot nu toe nog geen gebruik gemaakt. Een voorbeeld waarin de EU-wetgever onder meer B2G-gegevensdeling heeft gereguleerd is te vinden in de ITS-Richtlijn 2010/40 en de bijbehorende gedelegeerde Verordening over real-time verkeers-informatiediensten.⁵²

4. De data intermediary

In de gegevens economie en daarmee in gegevensdeling zijn nieuwe actoren in opkomst, wier rol en *data governance regime* mogelijk kunnen helpen bij het bevorderen van vertrouwelijke en wetsconforme B2G. Vaker genoemde voorbeelden zijn 'data trusts', 'data commons' of data cooperatieven'.⁵³ De terminologie voor deze actoren is buitengewoon dynamisch en sterk in ontwikkeling. Afgrenzings van de termen lijkt nog niet aan de orde. Toch kunnen binnen deze groep actoren enkele gemeenschappelijke kenmerken worden gedetecteerd. Het belangrijkste kenmerk is dat ze allemaal beogen op een of andere wijze een vertrouwelijke gegevensdeling tot stand te brengen die wordt vertrouwd door degenen die hun gegevens ter beschikking stellen voor deling enerzijds, en de ontvangers van die gegevens anderzijds. Zij beogen daarnaast degenen die hun gegevens beschikbaar maken enige vorm van controle te geven over de wijze waarop met hun gegevens wordt omgegaan. In B2G die centraal staat in dit paper zijn degenen die hun gegevens ter beschikking stellen bedrijven, en de ontvangers van gegevens gemeenten.

De term "data intermediary" biedt bij afwezigheid van eenduidige terminologie voor nu een overkoepelende term aan dit type entiteiten. Data intermediaries willen meer algemeen gegevens delen op een wijze die recht doet aan de rechten en belangen van degenen die hun gegevens ter beschikking stellen. In het geval van B2G gaat het om de bescherming van de rechten en belangen van bedrijven. Daarnaast kunnen data intermediaries vanwege hun onafhankelijkheid van degenen die gegevens ter beschikking stellen en van degenen die de gegevens ontvangen en gebruiken, mogelijk helpen bij het oplossen van tegenstrijdige of conflicterende belangen van de betrokken belanghebbenden bij het delen van de gegevens. Deze onafhankelijkheid moet net als een aantal andere afspraken worden bewaakt en vastgelegd in het hierna te bespreken data governance regime op basis waarvan de data intermediary gegevens van degenen die deze ter beschikking stellen kan delen.

⁵² Richtlijn 2010/40 van het Europees Parlement en de Raad van 7 juli 2010, Pb EU L 207/1 (6 augustus 2010) betreffende het invoeren van intelligente vervoerssystemen op het gebied van wegvervoer en voor interfaces met andere vervoerswijzen, die regels en voorwaarden vastlegt voor de invoering van Intelligente Transportsystemen, ofwel een systeem waarin communicatie- en informatietechnologie toegepast wordt voor wegvervoer, -infrastructuur, -voertuigen en -gebruikers. Art. 4 lid 5 verstaat onder ITS-dienstaanbieders ook particuliere aanbieders van ITS-diensten. Met de uitwisseling van informatie kunnen files verminderd worden, veiligheids- en andere digitale toepassingen in auto's beter werken en mensen gemakkelijker hun reis met het openbaar vervoer uitstippelen (uit: Kenniscentrum Europa Decentraal, Intelligente Transportsystemen ITS, 29 oktober 2022, <https://europadecentraal.nl/onderwerp/vervoer/intelligente-transportsystemen-its/>, bezocht op 27 maart 2024). Lidstaten kiezen zelf of zij een ITS invoeren. Zie ook Kennisplatform CROW, Real Time Traffic Information. Zie voor een duiding van de nieuwe RTTI gedelegeerde verordening voor wegbeheerders: https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/d397_real-time-traffic-information_nl.aspx, bezocht 27 maart 2024.

⁵³ Zie voor nadere uitwerking van deze termen H. Janssen & J. Singh, Data Intermediary (2022) Internet Policy Review (11) 1.

De belangrijkste belanghebbenden in een data intermediary ecosysteem ten behoeve van B2G zijn de data intermediary, de bedrijven, en de gemeente die de gegevens ontvangt, en indirect burgers wier gegevens, rechten en/of belangen kunnen worden betrokken of geraakt in B2G. Binnen een ecosysteem van een data intermediary beheert deze gegevens als afgesproken in het data governance regime, en biedt deze de bedrijven een zekere mate van vertrouwen in de manier waarop de gegevens zullen worden gebruikt.

In dit hoofdstuk worden bevindingen ten aanzien van de meest relevante eigenschappen van de data intermediary en van het data governance regime van een data intermediary toegelicht, en wordt verkend wat in de basis nodig is voor de ontwikkeling van een juridische blauwdruk voor gemeentelijke B2G die via een data intermediary zou moeten verlopen. Het hoofdstuk sluit af met een korte analyse van EU Data Governance Verordening die enkele regels stelt voor de erkenning van data intermediaries als organisaties die binnen de EU worden erkend. Deze DGA vertoont enige contouren voor wat betreft de normering van B2G, maar is op dit moment nog onvoldoende uitgekristalliseerd om te kunnen dienen als richtinggevend kader voor de ontwikkeling van B2G in gemeentelijke context.

4.1 Data governance

De term 'data governance' wordt veelal gedefinieerd als de uitoefening van zeggenschap en controle over het beheer van gegevens door het vastleggen en formaliseren van beslisrechten, en processen en controlemechanismen om die beslisrechten te effectueren.⁵⁴ In het data governance 'regime' van een data intermediary worden de specifieke, op de aan de orde zijnde B2G afspraken vastgelegd. Dit data governance regime steunt op een samenstel van juridische en organisatorische processen, en wordt in digitale omgevingen ondersteund door technische mechanismen. Het data governance regime heeft daarmee het karakter van een socio-technisch ecosysteem.⁵⁵ Het data governance regime moet in al zijn facetten voldoen aan alle relevante wettelijke eisen, ook aan sectorale wettelijke eisen die kunnen spelen in een specifieke (sectorale) B2G. Deze processen en mechanismen faciliteren, indien op de juiste wijze georkestreerd, een uitvoering van beslissingen, interventies, processen en enige vorm van controle door degenen die hun gegevens ter beschikking stellen – in de context van B2G veelal bedrijven.

4.1.1 Het data governance regime

Een data intermediary beheert en verwerkt gegevens zoals vastgelegd in het data governance *regime*. Dit regime legt vast op welke manier degenen die hun gegevens ter beschikking stellen (bedrijven), de data intermediary en de ontvanger (de gemeente) controle kunnen uitoefenen over de gegevensverwerking die nodig is om B2G te effectueren. De voorschriften behelzen veelal het opleggen van beperkingen aan bedrijven, aan de gemeente en/of de data intermediary zelf over de mogelijke interventies in de verwerking van de gegevens. Het data governance regime, en daarmee de

⁵⁴ R. Abraham, J. Schneider, J. Vom Brocke Data governance: a conceptual framework, structured review, and research agenda (2019) International Journal of Information Management (49) 424.

⁵⁵ J Singh and others, 'Responsibility & Machine Learning: Part of a Process' (27 October 2016) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2860048 bezocht op 14 mei 2024.

wijze waarop de beslismacht en controle over de gegevens tussen de betrokken actoren wordt verdeeld en met passende interventies is voorzien, varieert met het doel van de data intermediary, het type actoren dat gegevens beschikbaar stelt, het type gegevens dat wordt gedeeld, of bijvoorbeeld met het type ontvangers dat de gegevens gebruikt.

De precieze rol die een data intermediary inneemt bij het beschikbaar maken van data in B2G kan variëren. Een data intermediary kan, waar nodig, bedrijven begeleiden bij de gegevensverwerking, of bedrijven instrumenten zoals visualisaties bieden om de gegevensverwerking te volgen en te controleren. Door het aanreiken van controlemechanismen kan een data intermediary bedrijven een vorm van controle bieden over de verwerking van hun gegevens en het verdere gebruik ervan door de gemeente, zodat de bedrijven kunnen onderzoeken of de verwerking en het gebruik in overeenstemming zijn met hun rechten en belangen. De specifieke regulering van de omgang met de gegevens binnen het data intermediary ecosysteem worden vastgelegd in een data governance regime.

De mate van vertrouwen van bedrijven in het data governance regime hangt naast de afspraken in het dat governance regime zelf in de hoofdzaak af van het vermogen van het data intermediary ecosysteem de gegevens op een vertrouwelijke manier te verwerken en te beheren, en tegenstrijdige en mogelijk conflicterende rechten en belangen van belanghebbenden te voorkomen en zo nodig op te lossen. Een data governance regime moet duidelijke en effectieve instructies en interventies omvatten die de actor die indachtig het regime bekleed is met beslismacht en controle – de data intermediary en/of het bedrijf – in staat stellen om de gegevensverwerking effectief uit te voeren en te controleren.

Tegelijkertijd moet worden voorkomen dat één actor te machtig wordt – in de zin dat deze de rechten en belangen van de andere actoren terzijde kan stellen ten behoeve van het eigen belang. Actoren met controle over de gegevens moeten die gegevens op een wetsconforme, transparante en verifieerbare wijze beheren en controleren, zodat degenen die geen effectieve controle uitoefenen over de gegevensverwerking begrijpen wat er met de gegevens gebeurt, en dat de actor die controle heeft over de gegevens en die is bekleed met effectieve beslismacht, effectief ter verantwoording kan worden geroepen. Dit betekent dat een data governance regime effectieve *checks & balances* moet bevatten die ervoor zorgen dat het neerleggen van beslisrechten en controle over gegevens bij een actor worden ingeperkt door die actor verantwoordingsverplichtingen op te leggen jegens de andere actoren, alsook regels en mechanismen die (intern) toezicht effectief kunnen ondersteunen.

4.1.2 Overwegingen bij het data governance regime

Afhankelijk van de context waarin datadeling wordt gewenst, kunnen de specifieke kenmerken en details van de procedures en mechanismen binnen een data governance regime in een data intermediary ecosysteem sterk variëren. Uit de praktijk komen enige overwegingen naar voren die beschrijven welke activiteiten een data intermediary in elk geval zou moeten reguleren. De in eerdergenoemde *checks en balances* maken deel uit dergelijke activiteiten. In figuur 1 is een niet-limitatieve lijst opgenomen van onderwerpen die in het data governance regime van een data intermediary zouden moeten worden gereguleerd:

Fig. 1 Overwegingen die een generiek juridisch data governance regime zou moeten reguleren:

1. Welk(e) doel(en) een data intermediary nastreeft;
2. Op welke wijze de onafhankelijkheid van de data intermediary wordt geborgd;
3. Welk type data wordt verwerkt;
4. Welke type actoren (zowel degenen die delen en degenen die ontvangen) toegang tot het data intermediary systeem kan krijgen en wordt betrokken bij de gegevensverwerking;
5. Waar en op welke manier gegevens worden vastgelegd en opgeslagen;
6. Waar berekeningen en analyses worden uitgevoerd (gecentraliseerd bij de data intermediary, of gedecentraliseerd bij de bedrijven);
7. Welke actor de berekeningen en analyses uitvoert;
8. Welke actor de ruwe, bewerkte of (op bepaald niveau) geaggregeerde gegevens beschikbaar stelt aan de ontvanger;
9. Op welke wijze de kwaliteit van gegevens wordt gegarandeerd;
10. Op welke wijze de ontvanger de gegevens kan gebruiken, alsmede waar mogelijk controle op dat gebruik;
11. Op welke wijze taken en verantwoordelijkheden ten aanzien van de gegevensverwerking worden verdeeld tussen de partijen in het data intermediary ecosysteem;
12. Of en op welke wijze actoren kunnen interveniëren in de gegevensverwerking, en passende verwerkingsrestricties daarbij;
13. Mechanismen voor de documentatie, logging en visualisatie van de gegevensverwerking;
14. Welke maatregelen worden genomen om de regels van het data governance regime effectief op te leggen, en door wie de naleving wordt opgelegd;
15. Of en op welke wijze het gebruik van gegevens door de ontvanger kan worden gecontroleerd;
16. Op welke wijze interne conflicten voorkomen en zo nodig opgelost worden;
17. Op welke wijze beslissingen met betrekking tot gegevensverwerking worden verantwoord;
18. Impact assessments ter identificatie en mitigatie van risico's voor de (fundamentele) rechten en de veiligheid van degenen die hun gegevens ter beschikking stellen en van burgers op wie de verwerking betrekking heeft.

Het data governance regime in een data intermediary ecosysteem heeft zoals eerder vermeld het karakter van een 'socio-technisch ecosysteem' en niet van een louter 'technisch' ecosysteem. Een socio-technisch ecosysteem betekent dat in een data intermediary ecosysteem juridische mechanismen (het data governance regime, servicevoorwaarden voor de dienstverlening, wetgeving, contracten en fiduciaire plichten) en organisatorische processen (zoals autorisaties voor gegevenstoegang of de toewijzing van controle, toewijzing van specifieke verplichtingen en verantwoordelijkheden aan actoren met controle en beslistmacht) aanwezig zijn. De juridische en organisatorische mechanismen worden ondersteund door technische mechanismen die gegevensverwerking en-deling daadwerkelijk mogelijk maken.

Alle mechanismen – juridisch, organisatorisch en technisch – moeten op zodanige manier worden gereguleerd dat zij gegevensdeling faciliteren indachtig de rechten en belangen van alle betrokkenen, in het bijzonder die van degene die gegevens voor deling beschikbaar stelt, en worden geïmplementeerd en nageleefd. De rol van de data intermediary is het coördineren, beheren en,

afhankelijk van hetgeen het data governance regime voorschrijft, de verwerking van de gegevens (verzameling, opslag, analyses, verrijking en/of gegevensdeling met de ontvanger).

Het data governance regime van een data intermediary kan worden opgebouwd rond specifieke doelen. Hoewel doelen zullen variëren, zijn veel voorstellen voor data intermediaries op de één of andere manier gericht op het tegengaan van de machtsconsolidatie die vaak aanwezig is in de huidige gegevenspraktijken van online platforms en andere data-gedreven bedrijfsmodellen. In de praktijk lijken data intermediaries veeleer de toegang tot en het delen van gegevens op een andere manier te willen beheren en besturen, vaak als alternatief voor de huidige praktijk waarin online platforms en data-gedreven verdienmodellen de toegang tot en het gebruik van gegevens vrijwel exclusief beheren en controleren. De door data intermediaries beoogde 'herverdeling' van controle en zeggenschap over gegevens onderscheidt hen van de huidige reguliere gegevensverwerkingspraktijken.

Een voorbeeld van een entiteit die kenmerken draagt van een data intermediary in B2G-context is Amsterdam Data Exchange (AMdEX).⁵⁶ AMdEX bemiddelt bij het delen van gegevens; AMdEX onderzoekt manieren om het potentieel van gegevens en gegevensdeling in te zetten voor het welzijn van de samenleving als het "instrument om verantwoord gegevensgebruik te realiseren". AMdEX ontwikkelt technische componenten. AMdEX werkt enkel met metadata en verwerkt de data niet zelf. AMdEX werkt met executeerbare, geformaliseerde interpretaties van afspraken. Een belangrijke, nog onbeantwoorde vraag is hoe deze formele interpretaties door juristen gewaardeerd worden, hoe het proces naar de formalisering van de interpretaties zou moeten luiden, en hoe deze zouden kunnen worden ingebed. Ook is nog niet duidelijk welke terugkoppeling over de praktische toepassing juridisch kan worden verwacht.

4.2 Uitvoering

Het data governance regime reguleert in de hoofdzaak het controleren van de toegang tot en het gebruik van gegevens door de *ontvanger*; het data governance regime moet zodanig worden vormgegeven en afgestemd dat de activiteiten, instructies en interventies door actoren kunnen worden verwezenlijkt, terwijl de rechten en belangen van alle actoren, met name van degene die gegevens beschikbaar stelt voor deling, worden gerespecteerd. Hiertoe reguleert het data governance regime op welke wijze en door wie de volgende activiteiten moeten worden ondernomen:

- *Vastlegging en opslag van gegevens* van degenen die deze ter beschikking stellen. Het data governance regime van de data intermediary moet het verzamelen en opslaan van of anderszins toegang tot deze gegevens (in onbewerkte of geaggregeerde vorm) mogelijk maken, en aanwijzen wie deze taken zal uitvoeren;
- *Gegevensverwerking en -deling*, op een wijze zoals vastgelegd in het data governance regime. Het data governance regime bepaalt op welke manier waarde-extractie uit de gegevens kan worden gehaald, en schrijft voor hoe en door wie gegevens beschikbaar worden gesteld aan ontvangers, of op welke wijze de berekening en het gebruik van die gegevens en de resultaten daarvan door een ontvanger mogelijk worden gemaakt;

⁵⁶ <https://amdex.eu/usecases/>.

- *Transparantie* verwijst naar technische mechanismen die validatie, toezicht en controle faciliteren over de wijze waarop actoren met zeggenschap en controle over de gegevens, hun acties, en meer in het algemeen wat er met de gegevens gebeurt (zoals bijvoorbeeld is vereist in de transparantieverplichtingen in de AVG).

Deze activiteiten, de nodige instructies en eventuele interventies moeten worden geïmplementeerd op een manier die in overeenstemming is met de doelstellingen van de data intermediary en met de belangen van de actoren, al naar gelang de specifieke situatie. De wijze waarop dit plaats kan vinden wordt hierna op hoofdlijnen beschreven.

4.2.1 Vastlegging en opslag van gegevens

Gegevensverwerking en -deling via een data intermediary zal in de regel beginnen met een verzoek van een ontvanger voor een door de ontvanger gespecificeerd doel. Vanaf dat moment zal op een bepaald moment enige vastlegging en opslag van gegevens van degenen die hun data delen plaatsvinden. Het verzamelen van deze gegevens kan echter ook al beginnen voordat de een dergelijk verzoek was ontvangen, afhankelijk van wat het data governance regime hiervoor regelt. Het verzamelen en opslaan van gegevens kan ‘lokaal’ gebeuren, of bij de data intermediary zelf. Dat wil zeggen, gegevens kunnen worden verzameld en opgeslagen op de apparatuur van degene die de gegevens ter beschikking stelt, of in een opslaglocatie van de data intermediary. Waar het vastleggen en opslaan van de gegevens plaatsvindt hangt af van wat het data governance regime van de data intermediary voorschrijft.

Als gegevens worden vastgelegd en opgeslagen door de data intermediary, kan deze degenen die hun gegevens ter beschikking stellen technische stuurprogramma's aanbieden die de data intermediary in staat te stellen die gegevens vast te leggen. Zodra deze programma's op de juiste wijze zijn ingesteld kan een geautomatiseerde stroom van geselecteerde gegevens uit de gegevensbronnen (zoals bepaald in het data governance regime) naar de opslaglocatie van ofwel degene die zijn of haar gegevens ter beschikking stelt, ofwel van de data intermediary, op gang komen.

De servicevoorwaarden, en indien de AVG van toepassing is, het privacybeleid die in het data governance regime zullen moeten worden opgenomen, zullen de rechtsbasis op grond waarvan de gegevens mogen worden verzameld en opgeslagen. De servicevoorwaarden kunnen nader worden uitgewerkt en vastgelegd in overeenkomsten tussen de data intermediary en het betrokken bedrijf, of gebaseerd zijn op geïnformeerde toestemming als degene die zijn of haar persoonsgegevens ter beschikking stelt een natuurlijke persoon is. Naast contracten kunnen zogenoemde ‘fiduciare plichten’ van onverdeelde loyaliteit en zorgvuldigheid van toepassing zijn, en worden opgenomen in het data governance regime. Fiduciare plichten brengen wettelijke verplichtingen voor een data intermediary met zich mee en eisen dat een data intermediary volledig in het belang van degenen handelt die hun gegevens ter beschikking te stellen. Fiduciare plichten zijn van belang omdat contractuele afspraken enkel zien op de afspraken tussen de data intermediary en een bedrijf, terwijl er zich situaties kunnen voordoen die niet contractueel zijn beschreven en afgesproken. Voor die situaties kunnen fiduciare plichten aanvullend bescherming bieden aan degenen die hun gegevens ter beschikking stellen.

Om het vertrouwen en de instemming (contractueel of door middel van toestemming) van degenen die hun data ter beschikking stellen met het vastleggen en opslaan van gegevens te verkrijgen, moet

de data intermediary het specifieke doel beschrijven en mededelen waarvoor de gegevens worden vastgelegd, net als de bewaartermijnen en-voorwaarden, de typen gegevens die worden vastgelegd, welke specifieke juridische, organisatorische en technische mechanismen de rechten en belangen van degenen die hun data ter beschikking stellen, beschermen, welke verplichtingen er bestaan voor de data intermediary, alsook de wijze waarop de ontvanger aan die rechten en belangen moet voldoen, en de wijze waarop de naleving van deze rechten en belangen door de data intermediary worden afgedwongen.

Het data governance regime van een data intermediary zal bepalen welke actor – het bedrijf en/of de data intermediary – de gegevens zal bewaren. In de huidige ecosystemen bijvoorbeeld bepalen de servicevoorwaarden van online platforms meestal dat de gegevens van degenen die hun data ter beschikking stellen bij het platform blijven. De servicevoorwaarden van een data intermediary kunnen daarentegen bepalen dat de te verwerken gegevens zich ofwel bij de data intermediary, ofwel bij het bedrijf (of waar het om persoonsgegevens gaat, bij de natuurlijke persoon) bevinden.

4.2.2 Gegevensverwerking en -deling

Het data governance regime in het data intermediary ecosysteem stelt de ontvangers in staat de gegevens van degenen die ze ter beschikking hebben gesteld te gebruiken voor hun eigen doelstelling, die in overeenstemming dient te zijn met het data governance regime. Dit gebruik houdt veelal in dat waarde uit de gegevens wordt gehaald, in overeenstemming met de doelstelling van de data intermediary, zoals die is vastgelegd in zijn data governance regime (deze kunnen verder gedetailleerd worden in de servicevoorwaarden). Vaak wordt deze waarde gecreëerd door het uitvoeren van gegevensanalyses, door ontvangen gegevensbestanden te verrijken met andere gegevensbestanden, het afleiden van aggregaten en trends, door machinaal leren om voorspellings- of besluitvormingsmodellen te bouwen, etc.

Welke gegevensverwerking en gegevensdeling er ook plaatsvindt, deze moet geheel in overeenstemming zijn met het data governance regime, de servicevoorwaarden van de data intermediary, diens privacybeleid en andere informatiedocumenten, en zoals verder uitgewerkt in contracten of toestemmingsverklaringen. Data intermediaries kunnen technische mechanismen inzetten die waarde-extractie uit leveranciersgegevens mogelijk maken, mits deze inzet in overeenstemming is met het data governance regime, de servicevoorwaarden en geldende wetgeving. Data intermediaries kunnen ook juridische en technische mechanismen hebben die een gecontroleerde doorgifte van gegevens aan ontvangers mogelijk maken, of de die ontvangers in staat stellen om die gegevens (en de resultaten daarvan) te berekenen en te gebruiken, zolang het in overeenstemming met het data governance regime en met toepasselijke wettelijke plichten.

De gegevensoverdracht zelf houdt in dat één actor – degenen die de gegevens beschikbaar stelt of de data intermediary – de gegevens beschikbaar stelt aan de ontvanger. De ontvanger kan de gegevens gebruiken in overeenstemming met de toestemmings- en handhavingsmechanismen die aan die gegevens zijn gekoppeld. Deze toestemming- en handhavingsmechanismen hoeven niet noodzakelijkerwijs specifiek te zijn voor elke overdracht, ze kunnen ook vooraf gedefinieerd zijn.

De gegevensoverdracht kan zoals eerder beschreven in §2.4.2 ruwe gegevens omvatten, voorbewerkte gegevens betreffen, geaggregeerde gegevens betreffen, of een overzicht bevatten op basis van de resultaten van aggregaties over data van degenen (meer actoren) die hun gegevens beschikbaar stellen. De beslissing over welke gegevens beschikbaar zullen worden gesteld, wordt logischerwijze vastgelegd in het data governance regime van de data intermediary, en kan zo nodig in uitgewerkte vorm worden opgenomen in de servicevoorwaarden en in de contracten, en waar dat van toepassing is, in een privacy policy om degenen die hun data beschikbaar stellen te informeren voordat hun akkoord wordt verkregen voor de beoogde gegevensverwerking en-doorgifte.

Informatiedocumenten ter ondersteuning van de overeenkomst of toestemming moet op transparantie wijze weergeven welke gegevens en welk type gegevens beschikbaar (kunnen) worden gesteld aan de ontvanger, en op welke wijze de met de gegevens gemoeide rechten en belangen zullen worden beschermd wanneer de doorgifte plaatsvindt. Voor wat betreft persoonsgegevens stelt de AVG gedetailleerde transparantievereisten.

4.2.3 Transparantie van de gegevensverwerking

Data intermediaries zullen, als onderdeel van hun wettelijke transparantie- en auditverplichtingen, ook registraties en documentatie creëren en bijhouden over de interacties van de data intermediary met degenen die hun data beschikbaar stellen, en over andere activiteiten die plaatsvinden binnen het data intermediary ecosysteem. Deze registraties en documentatie kunnen van technische en niet-technische aard zijn. Wanneer het data governance regime bepaalt dat voor het bijhouden en documenteren van dergelijke registraties en documentatie technologie nodig is, kan het data governance regime technische maatregelen omvatten die logboeken, audits en/of visualisaties toegankelijk moeten maken voor de data intermediary en voor degenen die hun gegevens ter beschikking stellen zodat zij inzicht krijgen in de gegevensverwerkingen.

Deze mechanismen kunnen de verantwoordingsplicht en transparantie van de data intermediary verbeteren; ze kunnen degenen die hun gegevens beschikbaar maken (vooraf) inzage geven in de gegevensverwerking, gegevensoverdrachten, en/of hen in staat stellen verwerkingen die plaatsvonden in het verleden te inspecteren. Op basis van de bevindingen kunnen zij besluiten hun gegevens niet langer ter beschikking te stellen (en vervolgens hun toestemming of akkoord intrekken).

De informatie die voortvloeit uit deze inzichten zal de data intermediary in staat stellen om de voorkeuren voor de gegevensverwerking permanent te (her)overwegen en eventueel te (her)onderhandelen, net zoals voor de beperkingen die aan ontvangers worden opgelegd zoals vastgelegd in de servicevoorwaarden die de data intermediary afsprekt met de ontvangers. Ook degenen die hun gegevens beschikbaar stellen worden beter geïnformeerd wanneer ze toegang krijgen tot informatie over de verwerking van hun gegevens (bijv. via de resultaten van een risicobeoordeling door een tussenpersoon, via inzage in real-time logbestanden, audits of permanente monitoring, of via visualisaties), waardoor zij hun toestemming voortdurend kunnen (her)overwegen (en deze bijvoorbeeld kunnen intrekken), of kunnen overwegen om hun contract met de gegevensintermediair te ontbinden.

Transparantiemechanismen kunnen tot slot ontvangers informeren en hen in staat stellen om de gegevensverwerking door de data intermediary te inspecteren en te onderzoeken, waarbij dergelijke inspecties geheel in overeenstemming moeten zijn met de rechten en belangen van degenen die hun gegevens beschikbaar maken. Ontvangers kunnen met deze informatie (her)overwegen om opnieuw over de te ontvangen gegevens te onderhandelen of hun contract met de data intermediary voort te zetten.

4.3 Wettelijk kader bij B2G via een data intermediary (3P)

In deze paragraaf vatten we samen welke wetten van toepassing zijn wanneer een data intermediary betrokken wordt bij B2G. Een data intermediary faciliteert B2G op basis van een data governance regime dat in alle opzichten moet voldoen aan de wettelijke kaders die de rechten en belangen van de belanghebbenden beschermen. Zo moet bij B2G waarbij een data intermediary wordt betrokken de wetgeving als beschreven in §3 ('wettelijk kader bij B2G') voor zover van toepassing in een specifieke B2G worden nageleefd.

4.3.1 Data Governance act

De Data Governance Act ('DGA') is onlangs in werking getreden. Het belangrijkste doel van de DGA is het faciliteren van de data-economie in de EU; de DGA wil voorwaarden creëren voor het delen van gegevens op basis van een geharmoniseerd kader voor gegevensuitwisselingen binnen de interne markt van de EU. De DGA bevat drie pijlers om dit doel te bereiken; de twee meest relevante voor dit paper betreffen:

- Een meldsysteem en voorwaarden voor commerciële data intermediaries (DISPs), en
- Een registratiesysteem voor altruïstische data intermediaries.

Deze beogen twee 'typen' data intermediary te reguleren. DISP's streven een *commercieel doel* na en worden gereguleerd met een aantal voorwaarden waaraan zij moeten voldoen om in aanmerking te komen voor erkenning door de Europese Unie. DISP-diensten staan onder toezicht van een bevoegde overheidsinstantie die door de lidstaten worden aangewezen en die bevoegd zijn om boetes op te leggen en de bemiddelingsdiensten van een DISP stop te zetten wanneer er overtredingen plaatsvinden.

Data intermediaries die een *altruïstische doelstelling* nastreven dienen volgens de DGA te worden geregistreerd als rechtspersoon, en worden afzonderlijk gedefinieerd en gereguleerd door de DGA. Dit type data intermediary is gebaseerd op toestemming als het gaat om persoonsgegevens conform de AVG, of op de toestemming die een bedrijf geeft voor het verwerken van gegevens die geen persoonsgegevens betreffen – waarbij dit type data intermediary gegevens verwerkt *zonder* winstoogmerk. De vereisten voor het toezicht op de naleving lijken op de vereisten die gelden voor DISPs; de lidstaten wijzen toezichthoudende autoriteiten aan voor het toezicht op de naleving van de DGA.

Data intermediaries met een altruïstische doelstelling moeten formeel en functioneel onafhankelijk zijn van degenen die hun gegevens beschikbaar maken en van de ontvangers. Dit type kan zich laten registreren als 'erkende' data intermediary met een altruïstische doelstelling bij openbare registers van bevoegde overheidsinstanties. Eenmaal erkend kan deze data intermediary in de hele EU actief zijn. De Europese Commissie zal een 'Rulebook' ontwikkelen met technische, beveiligings- en informatievereisten en aanbevelingen over interoperabiliteit. De DGA richt een Europees Comité voor gegevensinnovatie (EDIB) op, dat naar verwachting zal samenwerken met het EU-toezichtorgaan voor gegevensbescherming en cyberbeveiligingsinstellingen, evenals met betrokken nationale overheidsinstanties.

B2G via een data intermediary valt waarschijnlijk binnen het domein van de data intermediary met een altruïstische doelstelling. Omdat de DGA tot zover voornamelijk procedurele contouren van dit concept geeft, lijkt het concept nog sterk in beweging. De DGA drijft voor zijn materiële juridische concepten op de AVG. Hoewel de Europese commissie inzet op de ontwikkeling van juridische concepten en regulering rondom dit type data intermediary die een belangrijke basis zullen leggen onder haar nog te ontwikkelen Rulebook, wordt in wetenschappelijk onderzoek al nagedacht over nadere invulling van minimumvereisten en voorwaarden voor gegevensdeling via een data intermediary.

In situaties waarin een niet-commerciële data intermediary wordt ingezet in B2G ten behoeve van (locale) overheden onderzoeken wij welke stappen gezet zouden moeten worden om een generiek juridisch-technisch data governance raamwerk te ontwikkelen die van toepassing zou kunnen worden in B2G-situaties. Bij het ontwikkelen van dit raamwerk moet worden onderzocht waar op dit moment juridische, organisatorische en technische vragen rijzen en waar machts- en controlevraagstukken met betrekking tot gegevensbeheer moeten worden gereguleerd, zodat degenen die hun gegevens voor deling ter beschikking stellen daadwerkelijk worden beschermd, en de (lokale) overheid en daarmee de (locale) samenleving kan profiteren van B2G die de wet en de rechten en belangen van alle betrokken actoren respecteert.

4.3.2 Juridische statuur van de data intermediary

De rol van de data intermediary met bijbehorende plichten en verantwoordelijkheden die worden vastgelegd in het data governance regime kan in beginsel worden vervuld door natuurlijke personen. De voorkeur gaat in de praktijk echter uit naar een data intermediary in de vorm van een rechtspersoon met het oog op het waarborgen van de gewenste onafhankelijkheid en de nakoming van wettelijke plichten en verantwoordelijkheden, met name wanneer de data intermediary meer structureel wordt betrokken wordt in B2G.

De DGA stelt een vijftal vereisten ten aanzien van data intermediaries voor data-altruïsme om in aanmerking te komen voor registratie in een openbaar nationaal register van erkende organisaties voor data-altruïsme. Twee van die vereisten kunnen meer richting geven aan beantwoording van de vraag welk type rechtspersoon voor data intermediaries in B2G-context passend is. Eén van de vereisten is dat een data intermediary voor data-altruïsme een rechtspersoon dient te zijn die op grond van het nationale recht is opgericht om doeleinden van algemeen belang zoals bepaald in het nationale recht te verwezenlijken. Een ander relevant vereiste is dat de rechtspersoon dient te werken

zonder winstoogmerk, en dat deze juridisch onafhankelijk moet zijn van enige entiteit met winstoogmerk.

De typen rechtspersonen naar Nederlands recht die op basis van voorgaande twee vereisten het meest voor de hand liggen zijn de *vereniging* (artikel 2:26 BW) en de *stichting* (artikel 2:285 BW). De naamloze vennootschap (nv) en besloten vennootschap (bv) hebben per definitie een winstoogmerk en zijn vooralsnog uitgesloten voor het type data intermediary dat centraal staat in B2G. De coöperatie is een speciale vorm van een vereniging, maar ook daarvoor geldt een winstoogmerk. Een coöperatie kan dit winstoogmerk uitsluiten, maar verdere bespreking daarvan reikt voor de huidige bespreking te ver. Veruit het grootste gedeelte van de rechtspersonen die zich in Nederland (nagenoeg) geheel inzetten voor het algemeen belang – het hierboven eerst besproken vereiste uit de DGA – zijn stichtingen, gevolgd door verenigingen.⁵⁷

Afhankelijk van de doelstelling en gewenste structuur zou de data intermediary aldus de vorm kunnen aannemen van een vereniging of stichting. Een vereniging kan voor data intermediaries als voordeel hebben dat de verschillende belangen die gemoeid zijn bij B2G op een meer democratische wijze vertegenwoordigd kunnen worden. De zeggenschap en de controle over de gegevens ligt overwegend bij de leden, doordat het zwaartepunt van de besluitvorming bij hen ligt. Leden hebben inspraak door middel van de stemrechten die zij uit kunnen oefenen in de algemene ledenvergadering.⁵⁸ Het bestuur wordt gekozen uit het midden van de leden.

Een *stichting* kent een meer hiërarchische structuur waarin de oprichters het stichtingsbestuur kiezen dat het beleid bepaalt. Een stichting heeft geen leden, maar doorgaans wel donateurs of subsidieverstrekkers die niet het beleid bepalen, maar die wel om verantwoording van het bestuur kunnen vragen over het gevoerde beleid.⁵⁹ Snelle besluitvorming is vermoedelijk gewenst bij een data intermediary. Zeker in de beginfase van de eerste B2G data intermediaries valt te verwachten dat zich vaak nieuwe situaties voor zullen doen waarvoor ontwikkelde statuten, beleidsplannen of governance regimes nog geen eenduidige handelswijze bieden. Een stichtingsbestuur dat in zo'n situatie direct een besluit kan nemen is effectiever, althans sneller, dan een verenigingsbestuur dat eerst de algemene vergadering moet raadplegen voordat een besluit kan worden genomen. Onder meer voor wat betreft efficiency zou een stichting dan de voorkeur verdienen boven een vereniging.

Verder onderzoek zal moeten uitwijzen welk type rechtspersoon het meest geschikt is voor een data intermediary die betrokken is bij B2G, waarbij gekeken moet worden naar de doelstelling van de data intermediary, het type gegevens dat wordt gedeeld, of de belangen van degenen die hun gegevens ter beschikking stellen overwegend heterogeen of juist homogeen zijn, welk toezicht nodig is, etc. De vormgeving van het data governance regime van de data intermediary is beslissend bij de keuze voor het type rechtspersoon. De hoofdregels van het data governance regime die de data intermediary reguleren zullen in de statuten van de rechtspersoon worden opgenomen; de uitwerking ervan kan volgen in onderliggende regels.

⁵⁷ R.H.F.P. Bekkers, G.J. van Leijenhorst en A.E.M. Leijten, 'Toezicht op Algemeen Nut', 30 mei 2022; B. Snijder-Kuipers, 'Omzetting als rechtsvormwijziging', (IVOR nr. 70) 2010/\$5.5.

⁵⁸ Art. 2:38 BW; Tekst & Commentaar BW, [commentaar op art. 2:26 BW](#): De gewone vereniging.

⁵⁹ [M.J. van Uchelen-Schipper](#), 'De rol en positie van de raad van toezicht van de stichting' (IVOR nr. 112) 2018/\$4.

4.4 Uitdagingen bij gegevensdeling in B2G via een data intermediary

Uitdagingen bij B2G waarbij een data intermediary wordt betrokken:

- Bij B2G wordt de doelbinding van een verwerking doorbroken (hetgeen onder voorwaarden toelaatbaar is); bijzonder is dat de doelbinding transformeert van privaatrechtelijke naar publiekrechtelijke context. Hoe kunnen de specifieke wettelijke vereisten bij die transformatie worden geborgd in een data governance regime?
- Een heterogene groep van stakeholders met uiteenlopende en soms conflicterende wensen/eisen die gegevens beschikbaar stellen kan leiden tot conflicterende belangen binnen het data intermediary ecosysteem; hoe kunnen deze tijdig en effectief worden geadresseerd in een data governance regime?
- Hoe kan effectief intern toezicht worden uitgeoefend op de activiteiten die plaatsvinden binnen het data intermediary ecosysteem en hoe moet dit beslag krijgen in het data governance regime; kan het type rechtspersoon hierbij mogelijk een oplossingsrichting bieden?
- Als een data intermediary ecosysteem met een bepaalde mate van efficiëntie wil functioneren zal tot op zeker hoogte moeten worden gewerkt met profielen. Hoe verhoudt zich het werken met profielen tot vereisten van transparantie en het voorkomen van discriminatie van personen?
- De binding en juiste duiding en afbakening van de taken, rollen en verantwoordelijkheden van de personen (*data stewards*) in een data intermediary bepaalt in welke mate de data intermediary, met name wanneer deze opereert vanuit een gecentraliseerde perspectief, kan komen tot wetsconforme en voorspelbare B2G. Dit vergt een doordenking van de kennis, vaardigheden en professionaliteit van deze personen.
- Kan voorkomen worden dat B2G3P wordt gebruikt om wettelijke verplichtingen waaraan de gemeente zich moet houden, te omzeilen?
- Kan voorkomen worden dat een specifieke B2G uiteindelijk leidt tot het gebruik van de gegevens door de gemeente voor strafvorderlijke- en fraudedetectie doeleinden?
- Hoe verhoudt zich B2G binnen een data intermediary ecosysteem met duurzaam gebruik van energie?

5. B2G3P-aspecten die in een generiek juridisch raamwerk aandacht behoeven

De aspecten die in een B2G data governance regime en daarmee waarschijnlijk in een generiek B2G data governance regime moeten worden geborgd (zie Fig. 1) moeten verder worden uitgewerkt:

- | |
|---|
| <ol style="list-style-type: none">1. Welk(e) doel(en) een data intermediary nastreeft;2. Op welke wijze de onafhankelijkheid van de data intermediary wordt geborgd;3. Welk type data wordt verwerkt; |
|---|

4. Welke type actoren (zowel degenen die delen en degenen die ontvangen) toegang tot het data intermediary systeem kan krijgen en wordt betrokken bij de gegevensverwerking;
5. Waar en op welke manier gegevens worden vastgelegd en opgeslagen;
6. Waar berekeningen en analyses worden uitgevoerd (gecentraliseerd bij de data intermediary, of gedecentraliseerd bij de bedrijven);
7. Welke actor de berekeningen en analyses uitvoert;
8. Welke actor de ruwe, bewerkte of (op bepaald niveau) geaggregeerde gegevens beschikbaar stelt aan de ontvanger;
9. Op welke wijze de kwaliteit van gegevens wordt gegarandeerd;
10. Op welke wijze de ontvanger de gegevens kan gebruiken, alsmede waar mogelijk controle op dat gebruik;
11. Op welke wijze taken en verantwoordelijkheden ten aanzien van de gegevensverwerking worden verdeeld tussen de partijen in het data intermediary ecosysteem;
12. Of en op welke wijze actoren kunnen interveniëren in de gegevensverwerking, en passende verwerkingsrestricties daarbij;
13. Mechanismen voor de documentatie, logging en visualisatie van de gegevensverwerking;
14. Welke maatregelen worden genomen om de regels van het data governance regime effectief op te leggen, en door wie de naleving wordt opgelegd;
15. Of en op welke wijze het gebruik van gegevens door de ontvanger kan worden gecontroleerd;
16. Op welke wijze interne conflicten voorkomen en zo nodig opgelost worden;
17. Op welke wijze beslissingen met betrekking tot gegevensverwerking worden verantwoord;
18. Impact assessments ter identificatie en mitigatie van risico's voor de (fundamentele) rechten en de veiligheid van degenen die hun gegevens ter beschikking stellen en van burgers op wie de verwerking betrekking heeft.

In dit onderzoek werd onderzocht welke juridische, organisatorische en/of technische belemmeringen en beperkingen het generieke juridisch-technische data governance model voor B2G zal kennen. De beperkingen werden onderzocht met behulp van verschillende onderzoeksmethoden:

- a. Analyse van wetgeving
- b. Juridische literatuur
- c. Interviews met organisaties die als data intermediary optreden
- d. Het bespreken van het onderzoek in twee workshops met stakeholders (bedrijven, FNW/IVI, IViR, ACM, gemeente Amsterdam)
- e. Informatie en ervaringen werden opgehaald uit de City Data Governance Conference (UvA/IViR & Tilburg University/TILT, Amsterdam 24 oktober 2024).

Annex met informatie over interviews, workshops en City Data Governance Conference volgen.