Reactie Bits of Freedom consultatie voorstel Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten.

Geachte ministers van Binnenlandse Zaken en Koninkrijksrelaties, en van Defensie,

Bits of Freedom waardeert dat er meer overzicht in de juridische systematiek is aangebracht door de verschillende wetten samen te voegen tot een overzichtelijke hoofdwet.

Inhoudelijk maken we ons echter zorgen. Op een algemeen niveau zien we een duidelijke trend vanaf de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2017 die zich doorzet in dit voorstel waarin de bevoegdheden van de diensten om gegevens te verzamelen en te verwerken worden verruimd terwijl de waarborgen worden verzwakt. Op dit punt is het voorstel uit balans. Hierdoor zijn burgers minder beschermd en komen zij steeds gemakkelijker op de radar van geheime diensten. Dit levert inbreuken op op de fundamentele rechten en vrijheden van individuele burgers. Daarnaast maakt Bits of Freedom zich ook zorgen over de druk die dit gebrek aan balans oplevert op de democratische rechtsstaat die het voorstel juist poogt te beschermen.

Hieronder zullen wij nader ingaan op een aantal concrete aspecten waar wij ons zorgen over maken.

Automatisering

De mogelijke mate van automatisering in dit voorstel is erg vergaand. De lijn die wordt uitgezet is te omschrijven als ‘automatisering, tenzij’. Er wordt expres voor het woord ‘automatisering’ gekozen omdat het zo veelomvattend is en dus heel veel dingen eronder (kunnen) vallen. Dat maakt de wet toekomstbestendig, maar ook weinig informatief en afgebakend. De term klinkt als het efficiënter maken van kleinschalige, interne werkprocessen maar houdt ook in dat de taken van de diensten mogen worden uitgevoerd door of met behulp van algoritmes en AI. Bij de automatisering wordt weinig aandacht besteed aan de risico’s die automatisering met zich meeneemt, of het introduceren van waarborgen om deze te mitigeren.

Waar wel waarborgen worden geïntroduceerd blijken die erg zwak. Voorgesteld artikel 36 bijvoorbeeld geeft een gedeeltelijk verbod op geautomatiseerde beslissingen. “De diensten starten geen inlichtingenonderzoek naar personen of organisaties uitsluitend op basis van geautomatiseerde resultaten”. Dat klinkt in eerste instantie als een aardige waarborg. Maar de toelichting laat er niet veel van over: “Bij deze handelingen kunnen wel geautomatiseerde resultaten worden gebruikt, maar alleen in combinatie met menselijke inbreng. Deze inbreng kán bestaan uit het verifiëren van de geautomatiseerde resultaten.”

Er mag dus geen inlichtingenonderzoek worden gestart op puur geautomatiseerde resultaten. Maar de vereiste menselijke inbreng bij die resultaten hoeft niet uit verificatie te bestaan. Dat betekent ook dat ongeverificeerde resultaten die overwegend uit de computer komen rollen wel

degelijk aanleiding kunnen zijn om een onderzoek naar personen of organisaties te starten.

Sommige soorten automatiseringstoepassingen worden gekwalificeerd als risicotoepassingen. Uit de omschrijving van deze toepassingen blijkt dat onder andere de inzet van gezichtsherkenningstechnologie hieronder valt. Voor de inzet van deze toepassingen geldt wel een verificatievereiste voordat op basis van deze resultaten toestemming wordt verzocht om een bijzondere bevoegdheid in te zetten of een onderzoek te starten. Wat we echter hebben gezien bij de toepassing van gezichtsherkenningstechnologie is dat mensen geneigd zijn om wat de computer zegt te bevestigen, ook als ze daar eigenlijk hun twijfels bij hebben, terwijl de computer echt niet altijd gelijk heeft.

Een andere voorgestelde waarborg bij de inzet van risicotoepassingen is dat de toepassing moet worden onderzocht op betrouwbaarheid. Naast dat dit niet betekent dat toepassingen met een verminderde betrouwbaarheid niet kunnen worden gebruikt, geldt de waarborg ook enkel ten aanzien van de toepassing. En niet ten aanzien van het gebruiuk ervan, bijvoorbeeld welke vraag aan een LLM gesteld wordt. Hoe groot de kans is op een fout-positief hoeft hier niet opgegeven te worden of mee te wegen. Daarnaast is de toets op betrouwbaarheid te beperkt, en laat het een weging op proportionaliteit achterwege. Dit heeft tot gevolg dat een LLM die precies doet wat verwacht wordt, maar veel meer data oplepelt dan eigenlijk nodig is volgens het protocol prima is om in te zetten. Dat schiet het doel voorbij.

Een toepassing is volgens het voorstel geen risicotoepassing wanneer deze in het maatschappelijk verkeer gebruikelijk is. Maar wanneer is iets in het maatschappelijk verkeer gebruikelijk? Daarnaast is de impact van het inzetten van een toepassing door de diensten een hele andere dan die door een burger. Deze andere impact neemt een hele andere verantwoordelijkheid met zich mee, die vraagt om een hele andere weging. Daarmee is dit criterium niet te gebruiken om te bepalen of een toepassing een risicotoepassing in de zin van deze wet moet zijn of niet.

Nu al blijkt uit rapportages van de toezichthouder dat de diensten kunstmatige intelligentie en geautomatiseerde data-analyse gebruiken zonder dat daarvoor (intern) voldoende kaders en waarborgen zijn ingericht. Een blanco en technologieneutrale voorziening om gebruik te mogen maken van technologie draagt niet bij aan een veilige en verantwoorde inzet van technologische middelen en vergroot de risico's op onrechtmatigheden.

Ter ondersteuning van de taakuitvoering

Voorgesteld artikel 38 regelt dat de diensten bijzondere bevoegdheden niet alleen voor hun taken mogen uitvoeren, maar ook 'ter ondersteuning van de taakuitvoering'. Dat is zorgwekkend omdat bijzondere bevoegdheden de bevoegdheden zijn waarvan is bepaald dat deze de vergaandste inbreuk maken op de rechten en vrijheden van burgers. Het is hen toegestaan deze in te zetten voor het doel om de nationale veiligheid en de democratische rechtsstaat te beschermen. De inzet van deze middelen is direct verbonden aan de taak van de diensten. Er kunnen niet zomaar extra rechtsgronden worden gemaakt om dergelijk ingrijpende bevoegdheden te kunnen inzetten. Al helemaal niet als er geen sprake is van extra inkadering en waarborgen, waar in dit voorstel niet in wordt voorzien. Met name lid 2 sub a en b baren Bits of Freedom zorgen.

Lid 2 sub a regelt de mogelijkheid om bijzondere bevoegdheden in te zetten om de uitoefening van operationele bevoegdheden mogelijk te maken. Dit geeft de diensten een ruimere mogelijkheid om te anticiperen op een toekomstige behoefte. Dat betekent eigenlijk dat de aanleiding om bevoegdheden in te zetten waarmee vergaand wwordt ingegrepen op de fundamentele rechten en vrijheden van burgers nog dunner kan zijn.

Lid 2 sub b regelt de mogelijkheid om bijzondere bevoegdheden in te zetten voor het ontwikkelen en onderhouden van capaciteiten die de diensten nodig hebben voor de taakuitvoering. Capaciteiten kunnen zowel menselijk als technisch zijn. Dat betekent dat het kan gaan om opleidingsdoeleinden van dienstwerknemers, het testen van nieuwe technologie of het trainen van eigen AI. De waarborgen die gelden voor risicobeheersing bij het inzetten van risicotoepasssingen gelden hier niet. Binnen dit regime gelden dus erg weinig waarborgen voor de inzet van bijzondere bevoegdheden en ongedefinieerde technologische toepassingen, die worden ingezet op echte data van echte mensen.

Toezicht

Bits of Freedom is blij te lezen dat er een samengesteld toezichtsorgaan wordt voorgesteld; het College van Toetsing en Toezicht. Ook vanuit de toezichthouders was in de aanloop naar het voorstel gecommuniceerd dat de optie voor geïntegreerd toezicht de voorkeur had. Helaas lijkt de manier waarop dit College is ingericht vooral een afbreuk van het toezicht op te leveren. Met name op de volgende punten ziet Bits of Freedom hier tekortkomingen in:

De toezichthouder wordt kleiner: Het aantal leden dat het toezicht moet gaan uitvoeren wordt met maar liefst 30% teruggebracht.

Bij de toetsingsverzoeken aan de voorkant is het effect daarvan vrij schrijnend: Die worden in principe in behandeling genomen door één enkel lid, slechts complexe verzoeken komen in aanmerking voor meervoudige behandeling door twee leden. Daarnaast geldt er een beslistermijn van maximaal twee weken. Bits of Freedom ziet hierdoor drie risico's ontstaan: Ten eerste is er hierdoor geen sparringspartner en maar een enkel perspectief. Ten tweede is een enkel individu kwetsbaarder voor externe druk. In het bijzonder wanneer er niet gepraat mag worden over de kwesties, wat bij toezicht op de geheime diensten het geval is. Ten derde ontstaat er een hoge (tijds)druk op de enkele persoon die binnen een tijdsspanne van twee weken op de verzoeken moet beslissen, wat kan afdoen aan de kwaliteit van de toets.

Daarnaast bepaalt voorgesteld artikel 48 lid 3 dat de toetsingscommissie haar oordeel moet vellen op basis van de gegevens die in het verzoek staan en de op grond van lid 2 verstrekte inlichtingen. Dat zou betekenen dat de toetsingscommissie eigen ervaringen uit het verleden niet langer mag betrekken in het komen tot haar oordeel. De commissie verliest hiermee als het ware haar geheugen. Daarnaast mogen bevindingen van de afdeling toezicht op deze manier ook niet worden meegenomen bij de toetsing en ontneemt het voorstel de toezichthouder de kans om te leren.

Ook het toezicht achteraf wordt teruggebracht, naar twee leden. Daarnaast wordt een proportionaliteitstoets geïntroduceerd op het inzetten van de bindende bevoegdheid van deze toezichthouder. De introductie van deze toets werpt een drempel op voor het inzetten van deze

bindende bevoegdheid die er niet zou moeten zijn. Immers, de toezichthouder krijgt juist bevoegdheden op in te grijpen waar dat noodzakelijk is. Zij moet kunnen handelen wanneer er een onrechtmatigheid is gevonden. Het werk van de geheime diensten is te belangrijk en impactvol om bij de toezichthouder bekende onrechtmatigheden te laten bestaan.

Voorgesteld artikel 164 maakt duidelijk dat het in dit voorstel niet gaat om geïntegreerd toezicht, maar om een College met verschillende afdelingen waartussen een strikte organisatorische scheiding bestaat. Dit werpt de vraag op of in de praktijk er meer of minder sprake is van integratie van het toezicht onder het nieuwe voorstel.De waarde van een geïntegreerd toezichtsstelsel ligt onder andere in het borgen van rechtszekerheid door de verschillende besluiten met elkaar in een lijn te laten zijn. Hiervoor is het van belang dat de toezichthouders onderling kunnen communiceren, gezamenlijk tot interpretaties en beslissingen kunnen komen en dat de oordelen van afdeling toetsing kunnen worden meegenomen in het toezicht en andersom.

Het aantal bevoegdheden waarop bindend toezicht wordt gehouden is verminderd. Voorgesteld artikel 47 geeft een beperkter aantal situaties waarin een bindende toets vooraf is vereist. En voorgesteld artikel 188 lid 1 omschrijft een beperkter aantal bevoegdheden waarop in bindend toezicht is voorzien.

Er wordt veel gebruik gemaakt van mandaatverlening en ondermandaat. Hiermee wordt het niveau waarop wordt geoordeeld of de inzet van een bepaalde bevoegdheid wel of niet noodzakelijk, proportioneel en subsidiair is steeds dichter op de operatie te liggen. Teamhoofden hebben zelf een directer belang bij het vervullen van onderzoeksopdrachten en kijken door hun functie meer vanuit een operationeel dan een rechtsstatelijk perspectief. Dit introduceert een groter risico op een operationele tunnelvisie.

Er is een eenzijdige hoger beroepsmogelijkheid geïntroduceerd tegen oordelen van de toetsingscommissie. Dat wil zeggen dat het een tweede kans is voor de diensten en de minister om een bevoegdheid toch te mogen inzetten ondanks het bezwaar van de toetsingscommissie. Een beroep in het belang van de bescherming van burgerrechten tegen een positief oordeel van de toetsingscommissie bestaat niet.

Staatsnoodrecht

In het uiterste geval kunnen onder het staatsnoodrecht zelfs veel van de verplichtingen op het gebied van toetsing, toezicht en verantwoording worden opgeschort. Hoewel het enerzijds prettig is dat in veel sectoren noodwetgeving beter in de wetgeving wordt verankerd, in een situatie dat die niet al acuut nodig is, gaat deze voorgestelde regeling wel erg ver. De voorgestelde regeling voorziet vooral in het buiten werking stellen van verantwoording en waarborgen, terwijl er ook regelingen te bedenken zouden zijn waarin in het uiterste geval deze zullen worden afgezwakt of uitgesteld. Ook mist op dit moment een regeling die afdwingt dat er zo snel mogelijk wordt teruggegaan naar een normale situatie die past bij een democratische rechtsstaat. Internationaal zien we vaker terugkomen dat wanneer er in landen eenmaal een noodsituatie is ingesteld het lang kan duren voordat weer wordt teruggegaan naar een normale situatie. Dat wil je voorkomen.

Hacken

Het voorstel deelt het hacken op in drie verschillende stappen. Enkel bij de laatste stap, het overnemen van de gegevens en het aanbrengen van voorzieningen, is een voorafgaande toetsing van de toetsingscommissie vereist.

In de eerste stap mogen de diensten, al dan niet met tussenkomst van het geautomatiseerd werk van een derde, binnendringen in een geautomatiseerd werk. Hierbij is het hen toegestaan om beveiliging te doorbreken. Nu hier niet langer voorafgaande toestemming voor vereist is, hoeven ook de technische risico's van de hackoperatie niet langer voorafgaand te worden opgegeven. Dat betekent dat er niet langer een externe toets plaatsvindt op de vraag of de technische risico's in verhouding staan tot het doel van de inzet en of het doel ook op een minder ingrijpende manier kan worden bereikt. Ook de vraag of de inbreuk op de rechten en vrijheden van de derde gerechtvaardigd kan worden door het doel van deze inzet wordt niet langer extern getoetst. Hierdoor ontstaat het risico op een operationele tunnelvisie.

De tweede stap is het bestendigen van de positie, het doen van onderzoek in het geautomatiseerd werk om het toestemmingsverzoek voor de laatste stap te motiveren en het treffen van voorbereidingen om de laatste stap mogelijk te maken. Hierbij wordt als het ware de digitale deur van de organisatie/persoon die wordt gehackt opengezet. Het openzetten van een dergelijke deur werkt nooit voor een enkele partij. Dat betekent dat wanneer de diensten door middel van het hacken deze deur openzetten ook andere, kwaadwillenden, makkelijker in deze digitale infrastructuur kunnen komen. Dit gaat ten koste van de veiligheid van deze infrastructuur. Gezien het hacken ook via zogenaamde derden mag, gaat dit niet alleen over de digitale deur van targets, maar ook over slachtoffers, dienstverleners of eventueel andere derden via wie de diensten bij het geautomatiseerd werk van een target zouden kunnen komen.

Evidente tegenstanders regime

Het voorstel kent een apart regime voor zogenaamde 'evidente tegenstanders'. Deze worden omschreven als (militaire) organisaties met offensieve doelen en activiteiten. Binnen dit regime geldt dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie gezamenlijk op verzoek van het diensthoofd een organisatie als evidente tegenstander kunnen aanwijzen. Deze aanwijzing wordt voor een bindend oordeel voorgelegd aan de afdeling toetsing. In het geval die oordeelt dat de aanwijzing rechtmatig is mogen jegens deze organisatie bijzondere bevoegdheden worden ingezet zonder voorafgaande toestemming. Dit geldt voor de periode van een jaar, maar mag telkens verlengd worden. Een organisatie wordt dus als het ware vogelvrij verklaard wanneer de aanwijzing als rechtmatig wordt beoordeeld.

Bij een zo vergaande maatregel verwacht je dat er echt kritisch wordt meegekeken. Maar hier wordt het extra pijnlijk dat de reikwijdte van de toets door de afdeling toezicht ver lijkt te worden ingeperkt. De toets moet plaatsvinden op basis van de voorgestelde artikelen die de definitie van '(militaire) organisaties met offensieve doelen en activiteiten' omschrijven. Dit is een erg beperkte toets die door de omschrijving in voorgesteld artikel 57 lid 2 geen ruimte over laat voor een proportionaliteitsweging door de toezichthouder.

Bij een dermate ingrijpende maatregel is het ook belangrijk dat organisaties niet lichtzinnig of

onterecht als evidente tegenstander aangewezen worden. De EU-besluiten waar naar verwezen wordt baseren opname van een organisatie op de lijst op het al dan niet zijn van *facilitator*, maar deze definitie is niet eenduidig. Ook laat voorgesteld artikel 56 lid 2 sub d de deur openstaan. Op basis hiervan kan een "organisatie die *wezenlijke* werkzaamheden verricht voor de ontwikkeling, vervaardiging, opslag, verwerving, proliferatie of verplaatsing van militaire middelen of de voorbereiding daarvan als militaire organisatie met offensieve doelen en activiteiten" worden aangewezen. Dit hoeft niet een buitenlandse partij te zijn, het is niet duidelijk wanneer de lat van 'wezenlijke' werkzaamheden geacht wordt te zijn gehaald, en deze 'wezenlijke werkzaamheden' hoeven ook niet de hoofdmoot te zijn van wat deze organisatie doet. Hierdoor vraagt Bits of Freedom zich af wat de grenzen voor deze aanwijzing zijn. Hoe groot moet de bijdrage zijn? Moet dit willens en wetens zijn gebeurd? En moet dit een groot deel van de activiteiten van de organisatie behelsen? Vallen grote (Nederlandse) hostingproviders hieronder in het geval dat zij in hun dienstverlening ook de opslag voor een buitenlandse hackgroep hebben gefaciliteerd? Zelfs als zij hier zelf niet van op de hoogte waren?

Uit juridische procedures die aangespannen worden door Muslim Rights Watch Nederland blijkt dat tientallen onschuldige Nederlanders voorkomen op terroristenlijsten. Dit zijn dan wel individuen en geen organisties. Maar het laat wel zien dat dergelijke lijsten geen onfeilbare bron zijn. En ook dat bepaalde groepen, zoals moslims of moslimorganisaties, een groter risico lopen om op deze lijsten te worden opgenomen. Bits of Freedom maakt zich zorgen over de risico's die de voorgestelde regels ten aanzien van evidente tegenstanders opleveren voor deze organisaties.

De Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma (Tijdelijke wet) moest later worden aangepast om aan Europees recht te voldoen door te voorzien in een voorafgaande, bindende toetsing bij de zogenaamde stomme tap. In dit voorstel wordt die voorziening voor zogenaamde 'evidente tegenstanders' ingetrokken. Hiermee lijkt opnieuw een strijdigheid met het Europees recht te ontstaan.

Het sleepnet wordt waar mogelijk verder verruimd

In 2017 stemde een meerderheid van de burgers tegen het voorstel van de Wet op de inlichtingen- en veiligheidsdiensten 2017. Deze wet werd niet voor niets in de volksmond de sleepwet genoemd. Dit was een verwoording van de grootste zorg over de wet: De massasurveillance die plaatsvond op grond van de bevoegdheid tot onderzoeksopdrachtgerichte kabelinterceptie. De term ging symbool staan voor ook de andere bevoegdheden waarmee de diensten in bulk data verzamelde. Na het duidelijke signaal van het referendum werden er een aantal toezeggingen gedaan en waarborgen toegevoegd. In dit voorstel worden juist die waarborgen geschrapt:

- Het gerichtheidscriterium "De uitoefening van een bevoegdheid dient zo gericht mogelijk te zijn." wordt geschrapt.
- De bevoegdheid tot verkennende kabelinterceptie uit de Tijdelijke wet verliest de beperking dat deze alleen voor de cybertaak kan worden ingezet.
- Data die met behulp van de bevoegdheid tot verkennende kabelinterceptie wordt verzameld mag met het buitenland worden gedeeld. Hierbij geld de voorwaarde dat deze gegevens niet voor andere doeleinden dan het vaststellen op welke gegevensstromen

een verzoek om toestemming voor de uitoefening van bulkinterceptie betrekking dient te hebben, ook voor de ontvangende partij. Deze buitenlandse partij valt echter buiten het toezicht, dus een echte waarborg geld hier niet.
- De eis uit de Tijdelijke wet om een omschrijving van de wijze waarop de reductie van gegevens binnen de gehele keten van verwerving invulling krijgt, vervalt.
- Er hoeft minder nauwkeurig te worden omschreven welke communicatiestromen worden getapt.
- De kenmerken die worden gebruikt als filters op de binnengehaalde data hoeven niet bij de toestemming te worden opgegeven, “omdat die kunnen meebewegen”.
- ‘Irrelevant verkeer’, zoals de data van streamingsdiensten etc, wordt niet langer uitgefilterd.
- Het wordt toegestaan om de bulkdata die door middel van kabelinterceptie is verzameld met behulp van AI te analyseren.

AI op bulkdata

Het voorstel geeft de diensten de bevoegdheid tot het geautomatiseerd bevragen van bulkdata. Onder huidige wetgeving moet hierbij vooraf goed worden aangegeven waar men precies naar kijkt. Nu stelt artikel 65 voor dat de minister een toestemming voor een jaar verleend om bulkdatasets te bevragen voor een thema zo breed als contra-terrorisme. Dit is zo goed als een blanco toepassing voor geautomatiseerde bevraging van bulkdata.

De verantwoording voor het geautomatiseerd bevragen van bijzondere bulkdata, waaronder bulkdata die is verzameld door middel van kabelinterceptie, is iets gedetailleerder tot het niveau van organisaties, personen of onderwerpen, maar nog steeds erg algemeen.

Einde relevantiebeoordeling

Artikel 27 Wiv 2017 regelde de relevantiebeoordeling. Daarin werd bepaald dat gegevens die verzameld zijn met een bijzondere bevoegdheid zo spoedig mogelijk op hun relevantie worden beoordeeld, en als dit niet binnen een jaar lukt de gegevens worden vernietigd. Dit vormde een waarborg voor burgers wiens gegevens als bijvangst in bulkdatasets zitten, dat deze data in elk geval binnen afzienbare tijd zouden worden vernietigd. Het nieuwe voorstel schrapt deze waarborgen en introduceert vele malen langere termijnen van twee jaar na het sluiten van een onderzoek en maximaal 10 jaar totdat het op relevantie wordt beoordeeld.

Verplicht data leveren

Voorgesteld artikel 94 stelt voor dat er voor de bescherming van *weerbaarheidsbelangen* een vordering kan worden gericht aan ‘een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken’. Dit kan iedereen zijn, dus ook een individuele ambtenaar of de systeembeheerder. Niet meewerken aan deze vordering wordt strafbaar gesteld. Dat maakt het een ingrijpende bevoegdheid, terwijl de term ‘weerbaarheidsbelangen’ onvoldoende is afgebakend. Afhankelijk van wie je het vraagt zijn we in oorlog met Rusland of niet, terwijl dit soort opvattingen van groot belang kunnen zijn voor de beoordeling of er wel/niet sprake is van weerbaarheidsbelangen in een gegeven situatie.

Samenwerkingen

Het voorstel verruimt de mogelijkheden voor de diensten om samenwerkingen aan te gaan. Voor meerdere van deze mogelijkheden gelden dezelfde bezwaren: Het delen van gegevens buiten het gesloten gegevenscircuit van de diensten brengt risico's voor de beveiliging hiervan met zich mee. Bovendien vallen de partijen waarmee een dergelijke samenwerking wordt aangegaan buiten het toezichtsregime van deze wet. Hiermee onttrekt een deel van de verwerking van gegevens of anderszins handelen dat bijdraagt aan de taakstelling van de geheime diensten zich aan het toezicht. Ook introduceert het een risico op een soort U-bocht. Waar het de diensten niet toegestaan zou zijn om bepaalde handelingen uit te voeren, zou dat op grond van dit artikel door een andere partij die niet aan hetzelfde toezicht is gebonden kunnen worden uitgevoerd, die de resultaten vervolgens deelt met de diensten op een manier die bij deze wet is voorzien. Vergelijkbare samenwerkingsmogelijkheden bestaan al in VK en VS, daar is veel kritiek op de beperkte controle op deze gegevensuitwisselingen, dat is ook hier voorzienbaar.

Vanzelfsprekend zijn we graag bereid om een toelichting te geven, mocht daar behoefte aan bestaan.

Met vriendelijke groet,
Namens Bits of Freedom,

Lotte Houwing