RAPPORT

Digitale Kroonjuwelen

Gegevens, documenten en registraties van Nationaal Belang

In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties

6 juni 2023

TwynstraGudde

Impact op morgen.

Samenvatting

Het belang van Nationale Belangen
In het kader van de voorbereiding van wetgeving waarin een gemeenschappelijke wettelijke grondslag voor de omgang met en het toezicht op informatieveiligheid wordt geregeld, is de volgende onderzoeksvraag gesteld: *Hoe moet worden omgegaan met de belangrijkste/gevoeligste overheidsprocessen en -informatie?*

Complexe maatschappelijke opgaven vragen steeds vaker om samenwerking in ketens en netwerken, waarin gegevens gezamenlijk worden gebruikt. Daartoe zullen steeds vaker gegevens bij de bron worden bewaard en uitsluitend daar bevraagd kunnen worden, in plaats van die gegevens steeds te verstrekken aan partijen die deze willen gebruiken in hun proces. Doordat dezelfde gegevens vervolgens een rol (kunnen) spelen in verschillende processen is het zaak dat deze adequaat beveiligd worden. Tegelijk verlangen burgers en bedrijven van de overheid betrouwbare informatie en betrouwbare dienstverlening. Daarvoor zijn betrouwbare, beschikbare en integere gegevens, documenten en registraties nodig. Voor de overheid is het van belang te weten over welke gegevens, documenten en registraties ze beschikt en deze duurzaam toegankelijk te houden en te beveiligen zodat betrouwbaarheid, integriteit en beschikbaarheid worden gegarandeerd.

Sommige gegevens (al dan niet vastgelegd in documenten en de registraties die gegevens en/of documenten bevatten) zijn van groter belang dan andere. Een beperkt aantal gegevens, documenten en registraties is voor overheid en maatschappij van zodanig belang dat ze als 'kroonjuwelen', of 'van Nationaal Belang' kunnen worden aangemerkt.

De staatssecretaris Koninkrijksrelaties en Digitalisering wil informatieveiligheid bij de overheid een wettelijke basis geven via een zorgplicht waaraan nadere regels kunnen worden gesteld, zoals de BIO[1]. Door het wettelijk verplichten van de BIO is de vrijblijvendheid voorbij. Door op één plaats een algemene zorgplicht voor informatieveiligheid bij de overheid te regelen wordt een vereenvoudiging van regels binnen de overheid bereikt. Daardoor komt de focus meer te liggen op het feitelijk beveiligen in plaats van administratief beveiligen. Bij een dergelijke zorgplicht past ook aparte aandacht voor de belangrijkste processen. Dat zijn niet alleen de vitale overheidsprocessen, dat kunnen ook andere 'kroonjuwelen' zijn. Voor deze 'kroonjuwelen' wil de staatssecretaris, samen met vitale overheidsprocessen en processen waar staatsgeheimen in rondgaan, een hogere mate van zorgvuldigheid bereiken. Als duidelijk is wat deze (digitale) 'kroonjuwelen' zijn die kunnen worden aangemerkt als 'van Nationaal Belang', dan kunnen aan organisaties, systemen en processen die gebruikmaken van die 'kroonjuwelen' eisen worden gesteld ten aanzien van beveiliging van deze digitale kroonjuwelen.

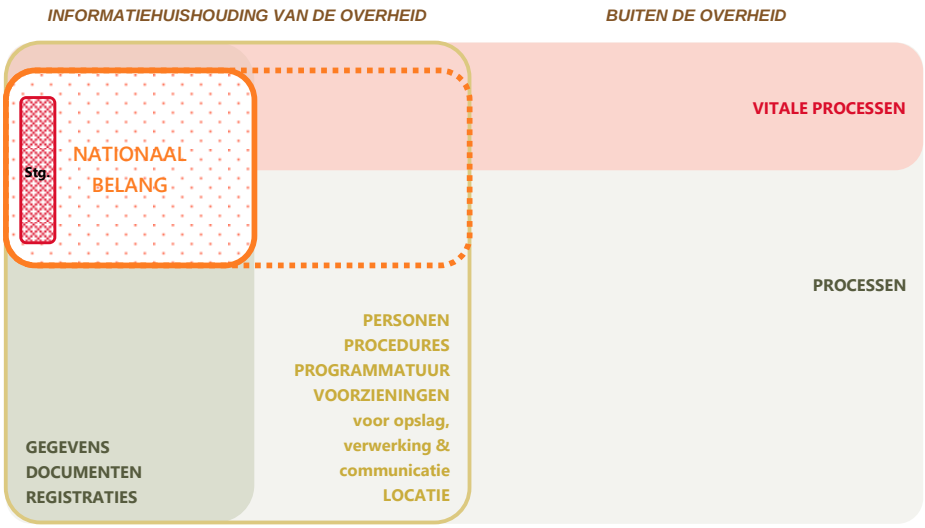
Deze analogie heeft als voordeel dat wordt aangesloten bij de ontwikkeling naar een federatief datastelsel en dat niet telkens hoeft te worden vastgesteld welke (delen van) veranderlijke processen en systemen van Nationaal Belang moeten worden verklaard. Verwerking van deze gegevens en documenten (soms uit registraties) is mogelijk voor alle overheden mits ze (en hun systemen) aan de vastgestelde eisen voldoen.

In Figuur 1 is de reikwijdte weergegeven van wat als 'Nationaal Belang' wordt aangeduid in dit onderzoek: het betreft gegevens, documenten en registraties binnen de overheid, waarbinnen in elk geval ook alle gerubriceerde gegevens, documenten en registraties vallen. Het Nationaal Belang zal deels overlappen met (gegevens, documenten en registraties in) in vitale overheidsprocessen, maar ook gegevens, documenten en registraties in niet-vitale overheidsprocessen

[1] Zie Tweede Kamerbrief 'Generiek kader voor vitale digitale processen van de overheid'.

kunnen tot Nationaal Belang behoren. De verwerking van gegevens, documenten en registraties van Nationaal Belang dient vanwege de hoogste mate van vertrouwelijkheid, beschikbaarheid en/of integriteit specifieke (extra) eisen te stellen aan personen, procedures, systemen, (fysieke) locaties voor opslag, etc.

In dit onderzoek wordt een methode gepresenteerd voor het afwegen van belangen gegeven om Nationale Belangen te kunnen identificeren. Daartoe zijn eenvoudige, onderscheidende criteria ontwikkeld. Vervolgens wordt aangegeven aan welke concrete maatregelen kan worden gedacht voor het verzekeren van de gewenste beveiliging (vertrouwelijkheid, integriteit en beschikbaarheid) van Nationale Belangen. Tot slot wordt aangegeven waaraan toezicht op Nationale Belangen zou moeten voldoen.



Figuur 1: Reikwijdte van Nationale Belangen

Afwegen van belangen

Er bestaat geen universele methode voor het afwegen van belangen. Ook wanneer gekeken wordt naar de methoden en werkwijzen voor het definiëren of afwegen van belangen binnen de overheid komt dit in de meeste gevallen neer op: "van belang is wat de organisatie van belang vindt". Dat gaat in veel gevallen in meer of mindere mate voorbij aan de waarde die buiten de organisatie kan worden gehecht aan specifieke belangen, zeker wanneer het gaat om gegevens, documenten en registraties die in toenemende mate éénmaal worden gemaakt en vervolgens worden (her)gebruikt door verschillende organisaties, overheidsorganisaties op alle lagen én organisaties en personen buiten de overheid, bovendien in geheel verschillende processen.

Dit onderzoek beoogt bij te dragen aan het ontwikkelen van een *generiek gemeenschappelijk kader* voor het kunnen bepalen welke gegevens, documenten en registraties kunnen worden aangemerkt als van Nationaal belang. Daarmee wil dit onderzoek belangen identificeren die naar hun *aard* belangrijk zijn, een *intrinsieke waarde* hebben en een zekere mate van onveranderlijkheid hebben. Door aan te sluiten bij intrinsiek belang in plaats van een afweging van belang, dreiging en weerstand (risicobenadering) én door te benadrukken dat het ziet op relatief onveranderlijke, herkenbare entiteiten waarvan het belang dat van een individuele overheidsorganisatie en -laag en zelfs dat van de gehele overheid overstijgt, komen we tot de volgende criteria:

Criteria voor gegevens, documenten en registraties van Nationaal Belang:

- Het betreft op zichzelf staande informatie-elementen of -objecten van de overheid: gegevens, documenten en registraties;
- Deze gegevens, documenten en registraties hebben een grote mate van onveranderlijkheid (wat niet geldt voor processen en systemen);
- Gegevens, documenten en registraties van Nationaal Belang hebben een intrinsiek belang voor meerdere of alle overheidsorganisaties, voor veel of alle burgers en bedrijven en/of zelfs voor de gehele Staat. Vanwege hun uniciteit, authenticiteit, vertrouwelijkheid, beschikbaarheid of een combinatie van die aspecten vormen ze een cruciaal element in het betrouwbaar en rechtmatig kunnen handelen van de Nederlandse Staat en/of de Nederlandse overheid en/of grote delen van de maatschappij. In geval van compromitteren of de mogelijkheid van compromitteren kan grote schade ontstaan voor de Staat, voor zijn bondgenoten en/of voor grote delen van de maatschappij.

Op basis van deze criteria kunnen de volgende categorieën gegevens, documenten en registraties worden onderscheiden:

- **Bijzondere (gerubriceerde) informatie**
  Alle bijzondere (gerubriceerde) informatie die valt onder het VIRBI 2013 of onder een internationaal verdrag of overeenkomst (van tenminste het niveau Stg.GEHEIM) en gegevens die zijn opgeslagen op een verboden plaats.
- **Nationale Basisregistraties**
  Alle nationale (basis)registraties - waaronder in elk geval alle basisregistraties – met een wettelijke basis, die cruciale, authentieke gegevens en/of documenten bevatten over personen, organisaties, gebouwen, geografie en economie. Ook de registraties met koppelgegevens, die gegevens van de ene registratie aan gegevens van een andere registratie koppelen, vallen hieronder als het om een koppeling met een registratie van Nationaal Belang gaat. Hierbij zijn ook de voorzieningen om deze registraties te raadplegen belangrijk. Deze voorzieningen (met een wettelijke basis) die gegevens raadplegen die van Nationaal Belang zijn, moeten voldoen aan een aantal vereisten.
- **Overige (documenten en) registraties van Nationaal Belang**
  Andere (documenten en) registraties kunnen volgens een systematiek identiek aan het afwegen van belangen van het Nationaal Archief ten aanzien van selectielijsten worden voorgedragen om ook te worden vastgesteld als Nationaal Belang.
- **Overige gegevens, documenten en registraties (al dan niet tijdelijk) op basis van een politieke belangenafweging**
  Naar aanleiding van een *politieke* belangenafweging kunnen overige gegevens, registraties en documenten van de overheid die door de Minister van BZK (ook tijdelijk) tot 'Nationaal Belang' worden verklaard. Dit heeft gelijkenis met de zgn. hotspot-monitor, alleen zullen hier andere criteria moeten worden aangelegd.

Het vaststellen van Nationale Belangen

Het vaststellen van welke gegevens, documenten en registraties worden aangemerkt als van Nationaal Belang geschiedt door de minister of staatsecretaris van het vakdepartement die het betreft in samenwerking met de minister van BZK. De minister van BZK stelt bovendien vast *dat* gerubriceerde documenten vanaf een bepaald rubriceringsniveau als Nationaal Belang worden aangemerkt én *wat* vervolgens de eisen zijn aan verwerken, verwerkers, systemen, locaties, etc.

Maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang

Ten aanzien van de maatregelen wordt aangesloten bij het VIRBI 2013, waardoor eisen gelden en maatregelen kunnen worden getroffen als aanvulling op het Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007) en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013), die ook onverkort van toepassing zijn. Er is wel een aanvulling nodig op wat het VIRBI 2013 voorschrijft – eventueel in een nieuwe regeling.

Deze aanvulling zou in elk geval, maar niet uitsluitend, moeten zien op:

- Definities – wat wordt verstaan onder gegevens, documenten/informatieobjecten en registraties, welke categorieën van verwerkingshandelingen worden onderscheiden;
- Reikwijdte: het betreft gegevens, documenten/informatieobjecten en registraties, het ziet op verwerking binnen de gehele overheid: naast de Rijksoverheid ook andere overheden en (semi-)publieke instellingen en hun uitvoeringsorganisaties;
- Beveiligingsbeleid: hoe het vaststellen van wat bijzondere informatie (of Nationaal Belang) verloopt, dat toestemming vooraf nodig is voor verwerking (inclusief *comply or ask permission*) en hoe centraal nationaal toezicht is ingericht;
- Eisen aan de beveiliging: beveiliging wordt niet langer louter ingericht op basis van risicomanagement, maar kent een aantal minimumnormen. Daarbij wordt niet alleen betrouwbaarheid, maar ook integriteit en beschikbaarheid opgenomen als algemene beveiligingseisen.

Een aantal mogelijke aanvullende concrete maatregelen die zien op standaarden, verplicht gebruik van overheidsvoorzieningen en aanbestedingen van ICT-diensten en ICT-producten zijn:

Concrete maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang:

- Gegevens, documenten en registraties van Nationaal Belang worden aangemerkt als bijzondere informatie: informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries, zoals gedefinieerd in het VIRBI 2013. Het VIRBI dient op enkele punten te worden aangepast en uitgebreid.
- Alle ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen, gelden de (open) standaarden van de 'Pas toe of leg uit-lijst', afwijken kan alleen na expliciete toestemming.
- Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Diginetwerk, Digipoort en Digikoppeling.
- Identificatie en authenticaties voor raadplegen van gegevens verloopt verplicht via DigiD.
- Voor aanbesteding van ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kunnen uitzonderingen op de Aanbestedingswet en de Aanbestedingswet op defensie- en veiligheidsgebied worden ingezet.

Daarnaast is nog een aantal concrete maatregelen voorstelbaar waarvan de mogelijkheid, wenselijkheid en haalbaarheid nader onderzoek vereist:

Aanbevelingen voor nader onderzoek naar concrete maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang:

- Onderzoek of het mogelijk en wenselijk is om specifieke locaties, zoals datacenters, aan te kunnen wijzen als verboden plaats.
- Onderzoek hoe bij ontwikkelen of aankopen van ICT-diensten en ICT-producten ten behoeve van opslag, verwerking en uitwisseling van gegevens van Nationaal Belang kan worden meegewogen hoe de afhankelijkheid van niet-Europese producten en diensten kan worden beperkt en verplicht mogelijkheden daartoe in aanbestedingen.
- Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht gebruik moeten maken van/ bestaan uit door het NBV geëvalueerde producten.
- Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht moeten worden ontwikkeld via een proces van Secure Software Development.
- Onderzoek hoe voor ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kan worden aangesloten op de ontwikkelingen in de Nationale Cryptostrategie.

Er dient nog wel een impactanalyse gemaakt te worden om te onderzoeken of de voorgestelde maatregelen in verhouding staan tot de gewenste niveaus van beveiliging en kwaliteitseisen enerzijds en de werkbaarheid anderzijds.

Toezicht op gegevens, documenten en registraties van Nationaal Belang
De reikwijdte van het belang van deze digitale kroonjuwelen voor de overheid en voor de maatschappij maakt bovendien dat centraal, nationaal toezicht noodzakelijk is om tot een adequaat en uniform niveau van beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens, documenten en registraties van Nationaal Belang te komen. Dat toezicht strekt over de Rijksoverheid en over andere overheden en (semi-)publieke instellingen en hun uitvoeringsorganisaties. Het toezicht strekt zich bovendien ook uit over de overheidsvoorzieningen die verplicht moeten worden gebruikt (ook voor het deel waarbij deze voorzieningen worden aangewend voor toegang of uitwisseling van andere gegevens dan gegevens van Nationaal Belang).

Voor toezicht op gegevens, documenten en registraties van Nationaal Belang zou het toezicht kunnen worden ingericht vergelijkbaar met het toezicht op de beveiliging van gerubriceerde informatie van de EU en NAVO. Daarbij wordt ingezet op een initiële accreditatie van de betreffende beveiliging bij de overheidspartijen *vóóraf*, aangevuld door periodieke inspecties.

Inhoudsopgave

Samenvatting 2

1. Inleiding 9

1.1. Onderzoeksvraag 13
1.2. Methode 13
1.3. Afbakening van het onderzoek 14
1.4. Definities 14
1.5. Leeswijzer 15

2. Zorgplicht vanuit diverse (wettelijke) kaders 16

2.1. Voor gegevens en informatie(systemen) 16
2.2. Voor gegevens in basisregistraties 17
2.3. Voor documenten 18
2.4. Voor digitale processen: NIS en straks NIS2 19
2.5. Tussenconclusie 20

3. Belangenafweging 22

3.1. Redeneerlijn voor Nationale Belangen 22
3.2. Afwegen van belangen bij archiefstukken 24
3.3. Te Beschermen Belangen in het BVA-stelsel 27
3.4. Belangenafweging in de BIO 29
3.5. Andere aanknopingspunten voor het identificeren en wegen van belangen 31
3.6. Criteria voor het afwegen van belangen 34
3.7. Wie stelt Nationaal Belang vast? 37
3.8. Tussenconclusie 40

4. Maatregelen 42

4.1. Gegevens, documenten en registraties van Nationaal Belang worden gelijkgesteld met bijzondere informatie cf. het VIRBI 2013 43
4.2. Fysieke locatie waar verwerking van gegevens, documenten en registraties van Nationaal Belang plaatsvindt 44
4.3. Gebruik van standaarden en toezicht daarop 45
4.4. Verplicht gebruik van voorzieningen voor uitwisseling van gegevens van Nationaal Belang 45
4.5. Aanbesteding van ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen 46
4.6. Geëvalueerde producten, Secure Software Development en de Nationale Cryptostrategie 48

4.7. Overige maatregelen 49
4.8. Strafbaarstelling 49
4.9. Tussenconclusie 49

5. Toezicht 51

5.1. Toezicht nu 52
5.2. Toezicht op de 'Kroonjuwelen' 53
5.3. Tussenconclusie Toezicht 54

6. Conclusies en aanbevelingen 56

6.1. Het belang van Nationale Belangen 56
6.2. Afwegen van belangen 56
6.3. Het vaststellen van Nationale Belangen 57
6.4. Het vaststellen van Nationale Belangen 59
6.5. Tot slot 59

Bijlagen 60

Bijlage 1: Wat te beschermen? – de veelheid aan begrippen 61
Bijlage 2: Interviewlijst 68
Bijlage 3: Bronnen 69

1. Inleiding

In de brief aan de Tweede Kamer over de *voortgang op informatieveiligheid bij de overheid* [2] van 18 maart 2021 heeft de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties een algemeen kader voor vitale digitale overheidsvoorzieningen toegezegd. In de brief aan de Tweede Kamer van 29 september 2022 over *Generiek kader voor vitale digitale processen van de overheid* onderscheidt de staatssecretaris van BZK binnen het totale complex van digitale overheidsvoorzieningen "vitale processen en andere 'kroonjuwelen'".[3] Een aantal voorzieningen van de digitale overheid is als *vitaal* aangewezen.[4] Voor vitale processen is - met het Besluit Beveiliging Netwerk en Informatiesystemen (Bbni) dat voortvloeit uit de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) van de minister van Justitie en Veiligheid (JenV) - al het nodige geregeld betreffende beveiliging. Dit onderzoek gaat over de "andere 'kroonjuwelen'" en verkent hoe zou moeten worden omgegaan met de belangrijkste/gevoeligste overheidsprocessen en -informatie. De uitkomsten vormen een bouwsteen voor het informatieveiligheidsvraagstuk van de eenduidige omgang met gegevens, documenten[5] en registraties[6] die van zeer grote waarde zijn voor de (decentrale) dienstverlening, alsook het organiseren van eenduidig toezicht daarop.

Een reden waarom het helpt om van 'kroonjuwelen' te spreken, is omdat 'kroonjuwelen' al een duidelijk eigenstandig belang en daarmee waarde vertegenwoordigen, ongeacht de context waarin ze zich bevinden. In monarchieën, worden alle juwelen die verbonden zijn aan het koningschap verstaan onder het begrip kroonjuwelen. Kroonjuwelen zijn hier *altijd* van waarde, of ze nou worden gedragen tijdens een officiële gelegenheid of niet. Kroonjuwelen hebben naast een intrinsieke ook een symbolische waarde en zijn het daarom waard extra beschermd te worden. Wanneer kroonjuwelen gebruikt worden bij een troonswisseling, worden voor vervoer naar en van de plek waar dit plaatsvindt, in Nederland in de Nieuwe Kerk in Amsterdam, en het verblijf van de kroonjuwelen, extra beveiligingsmaatregelen getroffen. Wanneer de kroonjuwelen tentoongesteld worden, dan zijn in het betreffende museum tijdelijk extra beveiligingsmaatregelen getroffen. En wanneer de kroonjuwelen in hun normale verblijf zijn, betreft dit een ruimte met specifieke maatregelen voor beveiliging en conditionering. Ofwel: niet het *proces* (vervoer, tentoonstelling, opslag) of *systeem* bepaalt beveiligingsmaatregelen, maar het feit dat het gaat om de *kroonjuwelen*. Indien gewone juwelen worden vervoerd, tentoongesteld of bewaard, dan gelden vrijwel altijd andere maatregelen en beveiligingseisen.

In dit onderzoek gebruiken we deze analogie voor de gevoeligste informatie van de digitale overheid: als we weten wat digitale 'kroonjuwelen' zijn, dan kunnen we voor processen die gebruikmaken van die 'kroonjuwelen' vaststellen aan welke (extra) eisen ten aanzien van beveiliging en toezicht deze moeten voldoen. Een voordeel van deze redenatie is dat 'kroonjuwelen' duurzamer zijn dan processen en systemen die veel veranderlijker zijn en omdat verschillende processen en systemen gebruikmaken van dezelfde 'kroonjuwelen', het overzichtelijk is voor processen en systemen welke beveiligingsmaatregelen in elk geval getroffen moeten worden. Gegevens, documenten en registraties hebben bovendien een eigen identiteit. Een "eigen identiteit" betekent dat ze een naam of identificatiekenmerk hebben,

[2] Voortgang informatieveiligheid bij de overheid, 18 maart 2021.
[3] Generiek kader voor vitale digitale processen van de overheid, 29 september 2022.
[4] Het overgrote deel van de als vitaal aangewezen processen van de sector Digitale overheid valt onder de Rijksdienst, zoals DigiD en Basisregistratie Personen (BRP).
[5] Waar we in dit rapport spreken van document wordt eigenlijk bedoeld: informatieobject. En informatieobject is een op zichzelf staand geheel van gegevens met een eigen identiteit. Voorbeelden van informatieobjecten/documenten zijn brief, e-mail, video, webpagina, tweet, subsidieaanvraag, vergunning. Zie: https://www.nationaalarchief.nl/archiveren/kennisbank/informatieobject.
[6] Registraties zijn databronnen met een wettelijke grondslag. Overheidsorganisaties hebben een wettelijke taak om bepaalde gegevens te verzamelen en te registeren in zogenaamde registraties. Een aantal registraties van de overheid is aangewezen als Nationale Basisregistratie. Deze basisregistraties zijn ook opgenomen in het overzicht van ruim 16.000 datasets op overheid.nl (https://data.overheid.nl/datasets), maar niet alle datasets hebben een wettelijk grondslag. We sluiten in dit rapport aan op de definitie van registratie en basisregistratie en gebruiken niet de bredere term dataset. Tegelijk zou een specifieke dataset op enig moment best van zodanig belang kunnen worden dat het wordt aangewezen als 'van Nationaal Belang'. Zie ook Bijlage 1.

waardoor ze te onderscheiden zijn. Hiermee kan een gebruiker eenduidig verwijzen naar een gegeven, document of registratie en zijn het bovendien herkenbare objecten waaraan een belang, een beveiligingsniveau en bijbehorende beveiligingsmaatregelen die de integriteit, vertrouwelijkheid en beschikbaarheid verzekeren, kunnen worden gekoppeld. Daarnaast, om in de analogie te blijven van deze kroonjuwelen, is van belang te verzekeren dat alleen geautoriseerden toegang hebben tot deze kroonjuwelen en dat navolgbaar is dat wijzigingen en aanvullingen op deze kroonjuwelen ook alleen zijn aangebracht door geautoriseerden[7].

Een classificatie van belangen biedt politici, beleidsmakers en andere betrokkenen houvast bij het bepalen of een bepaalde situatie als ernstig moet worden aangemerkt – en dus of de overheid haar verantwoordelijkheid dient te nemen en zo ja, op wat voor manier. Dit is eerder al gedaan voor vitale processen. Het is onmogelijk om alle processen van een samenleving voortdurend tegen alle dreigingen te beschermen. In de praktijk is daarom een onderscheid nodig tussen vitale en niet-vitale processen. Het Rijk heeft hiertoe een beoordeling uitgevoerd van de mate van vitaliteit van maatschappelijke processen, waarbij aan de gevolgen van uitval van deze processen een score is toegekend op potentiële economische, fysieke en sociaal-maatschappelijke impact. Daarnaast is ook gekeken naar cascadegevolgen. Door vitale processen aan te wijzen, probeert de overheid prioriteiten te stellen en ervoor te zorgen dat niet alle verstoringen als ontwrichtend worden gezien. Schaarse middelen zijn aldus effectief en legitiem in te zetten.[8]

Het 'vitale' karakter van maatschappelijke processen, zo stelt de WRR, is echter ook sterk afhankelijk van hoe deze processen in de praktijk zijn georganiseerd en van het risico op verstoringen. Dergelijke aspecten, inclusief de aanwezigheid van bijvoorbeeld terugvalopties en hersteltijden, zijn cruciaal voor de omvang van de schade of het aantal slachtoffers op het moment dat het misgaat. *Impact is met andere woorden geen onveranderlijke grootheid*, maar mede afhankelijk van de veerkracht van de partijen die verantwoordelijk zijn voor de vitale processen. Lijstjes met vitale processen kunnen dus van elkaar verschillen, van moment tot moment en ook per land. Op het terrein van het veiligheidsbeleid verlangen we van de overheid dat zij inzichtelijk maakt *welke belangen in het geding zijn*, aldus de WRR. Ook zal zij duidelijk moeten maken hoe de verdeling van lusten, lasten en risico's dient te zijn bij het behartigen van deze belangen en welke partijen waarvoor verantwoordelijk zijn.

De WRR wijst erop dat investeringsbeslissingen, overnames en de netwerkeffecten in de digitale wereld kunnen resulteren in grote en lastig te corrigeren afhankelijkheden[9]. Een belangrijke vraag is daarom welke voorzieningen of bedrijven we in Nederland willen houden (of: welke diensten we binnen de overheid willen (blijven) uitvoeren, met welke apparatuur en software de overheid zou willen werken, etc.), teneinde nationale belangen te beschermen. Meer dan nu het geval is zal de overheid dus moeten beschikken over de noodzakelijke kennis om de risico's van de nieuwe werkelijkheid vroegtijdig te kunnen duiden en 'ontwrichtingsbeleid' te kunnen formuleren. Een belangrijk onderdeel van dit beleid zal een beredeneerde afweging moeten zijn over de mate waarin we als land willen beschikken over terugvalopties, de mogelijkheid om systemen te isoleren en over voorzieningen die ook offline kunnen functioneren. En, zo kan in het kader van dit onderzoek worden toegevoegd, een afwegingssystematiek om te bepalen voor welke systemen en voorzieningen die terugvaloptie, in welke mate, zou moeten gelden.

De WRR adviseert om in aanvulling op het huidige Cybersecuritybeeld een *Cyberafhankelijkheidsbeeld* op te stellen, dat inzichtelijk maakt van welke partijen, digitale processen en diensten het functioneren van vitale processen in de Nederlandse samenleving afhankelijk is. Het zou een overzicht geven waarop ook het totale complex van digitale overheidsvoorzieningen, inclusief vitale processen en andere 'kroonjuwelen', inzichtelijk wordt. Dit afhankelijkheidsbeeld

[7] CIANA: naast Confidentiality, Integrity, Availability ook Non-Repudiation, and Authentication.
[8] Zie: WRR, *Voorbereiden op digitale ontwrichting* (rapport nr. 101, 2019).
[9] De WRR wijst er hierbij op dat bekend is dat talloze bedrijven en organisaties zeer afhankelijk zijn van de clouddiensten van slechts twee grote Amerikaanse aanbieders, Microsoft en Amazon. Hetzelfde geldt voor de afhankelijkheid van leveranciers van industriële controlesystemen, elektronische patiëntendossiers of geldautomaten.

zou niet in detail openbaar gemaakt kunnen worden gezien het gevoelige karakter van veel informatie. In het kader van dit onderzoek is aangegeven dat een dergelijk cyberafhankelijkheidsbeeld voor de overheid nog niet bestaat (hoewel veel gesprekspartners aangaven dat het goed zou zijn als het er zou zijn, maar ook dat het een enorme klus zal zijn om het op te stellen en te onderhouden).

Complexe maatschappelijke opgaven vragen steeds vaker om samenwerking in ketens en netwerken, waarin gegevens gezamenlijk worden gebruikt. Organisaties, ketens en processen maken (ook) gebruik van gegevens, documenten en registraties van de overheid. Veel van deze gegevens, documenten en registraties wordt in toenemende mate één keer opgeslagen en daarna – als bron – voor verschillende toepassingen, in verschillende processen gebruikt. Zie in dit verband bijvoorbeeld de beweging naar een federatief gegevensstelsel: de Interbestuurlijke Gegevensstrategie, die streeft naar de verantwoorde inzet van gegevens voor maatschappelijke opgaven, werkt aan realisatie van een federatief gegevensstelsel waarbij het uitgangspunt is dat gegevens bij de bron worden bewaard en uitsluitend daar kunnen worden bevraagd. Dat maakt dat deze gegevens(registraties) bij de bron van belang (kunnen) zijn voor meerdere organisaties, ketens en netwerken, waarmee hun intrinsieke waarde en het belang om deze gegevens(registraties) te beschermen toeneemt. Ze worden bovendien gekenmerkt door een grote mate van onveranderlijkheid: brongegevens, brondocumenten en basisregistraties moeten – ongeacht processen of systemen – steeds als onveranderlijke waarheid beschikbaar zijn en blijven voor die personen en organisaties die daar toegang toe hebben. Sommige van deze gegevens of registraties van de overheid kunnen een zodanig belang vertegenwoordigen dat ze als 'kroonjuweel', als van Nationaal belang kunnen worden aangemerkt.

De overheid heeft de plicht te zorgen dat deze gegevens, documenten en registraties beschikbaar, integer en vertrouwelijk zijn en blijven. Voor informatiebeveiliging[10] zijn deze maatschappelijke criteria vertaald in kwaliteitseisen ten aanzien van informatie en informatiesystemen. Bij de overheid worden deze begrippen als volgt gehanteerd[11]:

- *Beschikbaarheid*: betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot zowel de informatie en als de daaraan ten dienste staande, aanverwante bedrijfsmiddelen (informatiesystemen);
- *Integriteit*: het in overeenstemming zijn van gegevens, documenten en registraties met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen. Hiertoe behoren ook kwaliteitseisen voor registraties, waaronder in elk geval volledigheid, juistheid en actualiteit;
- *Vertrouwelijkheid*: het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder andere om het beveiligen van de toegang tot de gebouwen, informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, *trojan horses),* maar ook om maatregelen om te voorkomen dat de eigen medewerkers toegang krijgen tot informatie die niet voor hen is bedoeld.

Daarnaast moeten overheden, burgers en bedrijven bij interactie met gegevens, informatie en registraties van de overheid die deze als bron onder zich heeft ervan uit kunnen gaan dat zij daadwerkelijk met deze overheidsdienst te maken hebben en vice versa. Alvorens gegevens kunnen worden vrijgegeven of aanvaard, moet met een voldoende mate van zekerheid worden vastgesteld aan wie die gegevens worden verstrekt en van wie de gegevens afkomstig zijn. Dit vereist adequate elektronische *identificatie* en *authenticatie*. Vaak wordt authenticiteit ook kwaliteitseis gebruikt. Deze eis is minder relevant voor gegevens, documenten en registraties als zodanig – het krijgt relevantie bij een interactie met een gebruiker en/of ander systeem. We zien deze eis daarom veeleer van belang bij systemen waarin gegevens,

[10] De begrippen 'gegevens', 'informatie', 'registratie' en 'document' worden – naast andere aanpalende begrippen – in verschillende wet- en regelgeving, documenten en onderzoeken nogal eens door elkaar gebruikt (Zie ook bijlage 1). In dit onderzoek richten we ons met name op gegevens, documenten en registraties als mogelijk te beschermen 'kroonjuwelen'. In sommige verwijzingen zullen we toch ook 'informatie' gebruiken, omdat in de meeste wet- en regelgeving sprake is van 'informatiebeveiliging' in plaats van beveiliging van gegevens, registraties en/of documenten.
[11] Zie onder andere het Besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007), Stcrt. 2007, 122.

documenten en registraties worden verwerkt. Tegelijk levert de overheid een aantal voorzieningen voor identificatie en authenticatie van gebruikers die de beschikbaarheid van gegevens, documenten en registraties regelen en waarvoor – bij uitval – maar in beperkte mate alternatieven beschikbaar zijn. Dergelijke voorzieningen hebben ook zelfstandig een belang: hoewel ze niet uitsluitend worden gebruikt voor toegang tot belangrijke gegevens, documenten en registraties is de afhankelijkheid van veel overheden, burgers en bedrijven van deze voorzieningen groot.

De kwaliteitseisen beschikbaarheid, vertrouwelijkheid en integriteit worden bij digitale gegevensverwerking als uitgangspunten voor de informatieveiligheid gehanteerd. Het belang van gegevens, documenten en registraties bepaalt de eisen aan beschikbaarheid en met name de vertrouwelijkheid. Sommige gegevens, documenten en registraties zijn van een zodanig belang dat deze slechts aan een hele kleine, gedefinieerde groep gebruikers (burgers, bedrijven, overheden) toegankelijk wordt gesteld voor verwerking en/of alleen onder een heel zwaar regime kan worden gemuteerd en vernietigd. Aan het verwerken van deze bijzondere categorie gegevens, documenten en registraties, de 'kroonjuwelen', dienen de strengste eisen te worden gesteld.

In dit onderzoek duiden we de 'kroonjuwelen' aan als *Nationaal Belang*[12] en onderzoeken we hoe kan worden afgewogen welke gegevens, documenten en registraties kunnen worden aangemerkt als Nationaal Belang en wat voor een gemeenschappelijke wettelijke grondslag voor de omgang en het toezicht op informatieveiligheid voor die categorie kan worden geregeld. Voor de overheid is het zaak om – voor wat betreft de gegevens, documenten en registraties die ze zelf maakt of beheert – te bepalen wat de mate van belang ervan is, zodat duidelijk wordt welke eisen aan het gebruik moeten worden gesteld. Het moet duidelijk zijn welke gegevens, registraties en documenten vallen onder de categorie Nationaal Belang, welke maatregelen (afsprakenstelsels) dan van toepassing zijn en hoe de overheid vervolgens het toezicht op naleving van deze maatregelen inricht. Het uitgangspunt van dit onderzoek is dat het *niveau van te beschermen belangen* van gegevens, documenten en registraties eisen stelt aan de systemen, processen en applicaties waarbinnen deze worden gebruikt. Dat kunnen ook bijvoorbeeld processen zijn buiten de Rijksoverheid. Op dit moment bestaat al wel een kader voor bijzondere informatie (VIRBI 2013), maar deze is alleen gericht op verwerking van bijzondere informatie binnen de Rijksoverheid. Bovendien dient toezicht op een goede uitvoering van het VIRBI-kader plaats te vinden door en binnen het departement waar verwerking van bijzondere informatie plaatsvindt. Dit maakt het niet mogelijk ook eisen te stellen aan en toezicht te houden op een overheidsorgaan buiten het eigen departement en helemaal niet als het een medeoverheid betreft, indien bijzondere informatie wordt gedeeld met dit andere overheidsorgaan.

Uitgaande van de hiervoor beschreven redeneerlijn dat het beveiligingsniveau wordt bepaald door het belang van het gegeven, de registratie of het document én dat steeds vaker wordt samengewerkt in ketens en netwerken, waarin gegevens door meerdere organisaties en functionarissen worden verwerkt, is het niet wenselijk dat het delen van bijzondere informatie op dit moment wordt gehinderd door het bestaande kader. Ook daarom is het van belang opnieuw te bezien welke gegevens, documenten en registraties van Nationaal Belang zijn, hoe – onder welke voorwaarden – deze kunnen worden gedeeld en hoe toezicht daarop zou kunnen worden ingericht.

[12] Nationaal Belang is een werktitel, aangereikt door het ministerie van BZK als opdrachtgever van dit onderzoek. Het staat BZK uiteraard vrij om digitale 'kroonjuwelen' uiteindelijk met een andere term aan te duiden.

1.1. Onderzoeksvraag

In het kader van de voorbereiding van wetgeving waarin een gemeenschappelijke wettelijke grondslag voor de omgang met en het toezicht op informatieveiligheid wordt geregeld, is de volgende onderzoeksvraag gesteld:

Hoe moet worden omgegaan met de belangrijkste/gevoeligste overheidsprocessen en -informatie?

Het ministerie van BZK heeft als opdrachtgever voor dit onderzoek aangegeven dat hierbij geldt dat substantiële uitval van vitale systemen en van de belangrijkste/gevoeligste overheidsprocessen en -informatie leidt tot (in)directe schade aan de overheid en/of maatschappelijke schade, in omvang vergelijkbaar is met het in verkeerde handen vallen van informatie die is gerubriceerd als Stg.GEHEIM.

Het onderzoek diende antwoord te geven op de volgende deelvragen:

- Welke eenvoudige en onbetwiste criteria leiden tot een nationaal belang?
- Welke concrete eisen moeten aan het risicomanagement worden gesteld?
- Welke concrete maatregelen kunnen worden toegekend aan alle processen en informatie van nationaal belang?
- Wat betekent dit voor toezicht en accreditatie?

Verder heeft BZK aangegeven dat de antwoorden zodanig dienden te zijn dat ze in wetgeving kunnen worden vertaald: zo concreet en ondubbelzinnig mogelijk. En ten aanzien van de concrete eisen aan het risicomanagement betekent dit dat extern kan worden getoetst of een organisatie risicomanagement heeft toegepast dat voldoende betrouwbaar is voor het belang dat moet worden beschermd. Verder was de wens ten aanzien van de concrete maatregelen voor alle processen en informatie van nationaal belang, dat het abstractieniveau zodanig dient te zijn dat verdere precisering of keuzes het beschermingsniveau van de maatregel niet onaanvaardbaar aantast.

In dit rapport is gekozen voor ‘gegevens, documenten en registraties’ in plaats van voor ‘informatie en processen’ – de achtergrond hiervan wordt uitvoerig toegelicht. Ook is gekozen voor het ontwikkelen van een belangenafweging in plaats van (een bestaande, aangepaste of nieuwe methode van) risicomanagement. De reden daarvoor is dat om belangen te identificeren een risicoanalyse niet geschikt is: een risico is de resultante van belangen, dreigingen en weerbaarheid (zie ook hoofdstuk 3). Daarnaast is gekozen om voor geïdentificeerde Nationale Belangen uit te gaan van minimumeisen en -maatregelen, naar analogie van het VIRBI 2013. Uiteraard is het goed om na het bepalen van minimumeisen en -maatregelen en/of het implementeren daarvan na te denken over waar (nieuwe) kwetsbaarheden of risico’s zijn of kunnen ontstaan. Daartoe zijn talloze risicomanagementmethoden en -technieken beschikbaar; de belangrijkste eis aan risicomanagement is dat dit uniform van opzet is en dat dit uniform wordt uitgevoerd.

1.2. Methode

Voor dit onderzoek zijn diverse openbare bronnen en overheidsdocumenten geraadpleegd. Verder is gesproken met 30 personen van verschillende organisaties die betrokken zijn of moeten zijn bij dit onderwerp. Nadat ongeveer met de helft van de respondenten gesproken was, is een eerste brainstormsessie gehouden met een klankbordgroep bestaande uit vertegenwoordigers van de Rijksoverheid, provincies (departementen, uitvoeringsorganisaties, toezichthouder), gemeenten (VNG), waterschappen (UvW). Na deze bijeenkomst is een tussenrapportage opgesteld en de uitkomsten hiervan zijn getoetst bij de klankbordgroep. De reflecties, aanvullingen en suggesties voor verbetering die zijn opgehaald, bij de klankbordgroep en tijdens diverse voortgangsoverleggen met de opdrachtgever, zijn verwerkt in deze eindrapportage.

1.3. Afbakening van het onderzoek

Dit onderzoek richt zich op gegevens, documenten en registraties die de overheid – Rijksoverheid en medeoverheden – zelf opstelt, beheert en beschikbaar stelt. Hoe de technische werking van informatiesystemen in elkaar steken en/of welke processen hierbij komen kijken, valt buiten de scope van het onderzoek. Wat wel van belang is, zijn de vragen welke generieke (beveiligings-)maatregelen moeten worden getroffen ten aanzien van de informatiesystemen waarmee gegevens, documenten en registraties worden verwerkt en waarmee ze beschikbaar worden gesteld en/of uitgewisseld.

Dit onderzoek richt zich met name op gegevens, documenten en registraties: deze zijn relatief onveranderlijk, hebben een intrinsieke waarde en vertegenwoordigen daarmee een intrinsiek belang én zijn duidelijk te onderscheiden digitale objecten waaraan eisen en maatregelen zijn te verbinden (wat voor abstracties als 'processen' en 'informatie' veel lastiger is).

Aanvullend is onderzocht welke voorzieningen door de overheid worden geleverd die cruciale schakels vormen voor de beschikbaarheid van (belangrijke) gegevens, documenten en registraties. Een *voorziening* (zoals MijnOverheid, DigiD en Digipoort) is een informatiesysteem opgebouwd uit applicaties, configuraties, data en ICT-infrastructuur.[13] De moeilijkheid met voorzieningen ligt precies daarin: het is, net als informatie, een minder scherp afgebakende entiteit waardoor aspecten als begrenzing, eigenaarschap, aard en eigenschappen diffuus zijn. Bij Logius bijvoorbeeld wordt de veelvormigheid van het begrip 'voorziening' goed duidelijk in de opsomming die wordt gegeven van voorzieningen die worden aangeboden in het domein 'toegang': die reiken van DigiD, het Machtigingenregister en de Centrale OIN Raadpleegvoorziening (ook een register). Voor zover dergelijke voorzieningen als cruciaal kunnen worden aangemerkt voor de vertrouwelijkheid, integriteit en beschikbaarheid van de belangrijkste gegevens, documenten en registraties is daar iets over gezegd.

1.4. Definities

De begrippen gegevens en informatie worden in verschillende wet- en regelgeving door elkaar gebruikt, dat geldt ook voor de begrippen registratie en document. Een *document* is een geheel van gegevens, wat dus in theorie ook een registratie zou kunnen zijn. Een *registratie* is een bestand van gegevens, maar zou heel goed ook een bestand van documenten kunnen zijn. En zowel een gegeven, een document als een registratie zou kunnen worden aangemerkt als bijzondere informatie en dus van een rubricering kunnen worden voorzien. Dat laatste is in dit verband cruciaal, want daarmee kan dus een afweging gemaakt worden over *het belang* van zowel gegevens, informatie, documenten als registraties. Net als de begrippen 'gegevens', 'informatie', 'registratie' en 'document' worden ook 'informatiesysteem' en 'informatiehuishouding' naast en door elkaar gebruikt. Een overzicht van verschillende begrippen en definities is te vinden in bijlage

Ook de problematiek van beveiliging van gegevens, documenten en registraties (en processen, systemen, voorzieningen – zie hierboven – en nog meer) zou erbij gebaat zijn dat in wet- en regelgeving én in het dagelijks gebruik binnen de overheid uniforme, eenduidige en goed afgebakende begrippen en definities worden gebruikt. Het is gelet hierop en voor het komen tot een heldere afbakening van wat binnen Nationaal Belang valt cruciaal dat in wet- en regelgeving én in het dagelijks gebruik eenduidige, heldere en goed afgebakende begrippen en definities worden gebruikt. Het naast en door elkaar gebruiken en verschillende definities van begrippen kan (zal) tot verwarring en onduidelijkheid leiden voor de personen die met die wet- en regelgeving en dat beleid moeten werken. De aangekondigde Algemene

[13] Adviescollege ICT-toetsing, *Definitief Advies Logius ICT-infrastructuur* (12 april 2023), p. 9 (zie: https://www.adviescollegeicttoetsing.nl/binaries/adviescollegeicttoetsing/documenten/publicaties/2023/04/12/advies-logius-ict-infrastructuur/Advies+Logius+ICT-infrastructuur.pdf).

informatiewet beoogt meer samenhang te brengen tussen de wetgeving over informatievoorziening en -huishouding op diverse beleidsterreinen en een aantal generieke informatiewetten en -regelingen zou hieraan wellicht kunnen bijdragen.[14]

1.5. Leeswijzer

Dit onderzoek is als volgt opgebouwd. In Hoofdstuk 2 wordt beschreven hoe de zorgplicht voor informatiebeveiliging momenteel voor gegevens, documenten en registratie is geregeld. Het hoofdstuk biedt een overzicht van bestaande (nationale) wet- en regelgeving, inclusief bestaande afspraken- en normenkaders. Hoofdstuk 3 beschrijft bestaande werkwijzen voor het afwegen van belangen en komt tenslotte met een voorstel voor criteria voor het afwegen van Nationale Belangen. In Hoofdstuk 4 worden vervolgens maatregelen beschreven voor het veilig verwerken van gegevens, documenten en registraties van Nationaal Belang, plus een aantal mogelijke maatregelen waar nader onderzoek voor nodig is. In Hoofdstuk 5 is beschreven hoe het toezicht momenteel geregeld is en wat de wenselijke situatie zou zijn voor gegevens, documenten en registraties van Nationaal Belang. Ten slotte volgen in Hoofdstuk 6 conclusies en aanbevelingen uit dit onderzoek.

[14] Zie:https://ibestuur.nl/artikel/regeringscommissaris-algemene-informatiewet-zo-snel-mogelijk-naar-ministerraad/.

2. Zorgplicht vanuit diverse (wettelijke) kaders

Er zijn al verschillende (wettelijke) kaders opgesteld voor (het verwerken van) gegevens en de verwerking daarvan in informatiesystemen, inclusief het bewaren, beschermen en vernietigen ervan. Deze vormen een nadere invulling van de zorgplicht van de overheid voor gegevens, documenten en registraties. Voorzieningen die zijn aangemerkt als *vitaal* vallen onder het Bbni, dat voortvloeit uit de Wbni. Dit onderzoek richt zich op de vraag hoe de overheid moet omgaan met de andere gevoeligste en belangrijkste gegevens, documenten en registraties van de overheid. Deze zijn exclusief en de vraag in dit hoofdstuk is welke (wettelijke) kaders momenteel al 'iets' beschrijven hoe om te gaan met verschillende categorieën gegevens, documenten en registraties. Risicomanagement en proportionaliteit zijn bij bestaande regelgeving vaak het uitgangspunt om te komen tot een niveau van beveiliging en te treffen maatregelen. Enkele relevante (wettelijke) kaders worden hieronder beschreven, waarbij de kanttekening gemaakt moet worden dat deze opsomming zeker niet uitputtend is; de opsomming is echter wel illustratief voor de veelheid, verscheidenheid en ruimte voor interpretatie die bestaande wetgeving biedt.

2.1. Voor gegevens en informatie(systemen)

De **Baseline Informatiebeveiliging Overheid** (BIO)[15] beschrijft het basisniveau voor *informatie*beveiliging voor de beveiliging van (informatie)*systemen* van de overheid. Het is een normenkader gebaseerd op de internationale norm ISO 27001/2 en wordt gehanteerd binnen de Nederlandse overheid, het Rijk, Gemeenten, Waterschappen en Provincies. Het biedt een gezamenlijke taal voor alle overheidsorganisaties en een concretisering van een aantal normen die verplicht door alle bestuurslagen moeten worden nageleefd. De implementatie van de BIO blijft de verantwoordelijkheid van de overheidsorganisaties. Om hen daarbij te ondersteunen heeft het ministerie van Binnenlandse Zaken een ondersteuningsprogramma ingericht bij het Centrum voor Informatiebeveiliging en Privacybescherming (CIP).

Met de BIO kan het lijnmanagement verantwoordelijkheid nemen ten aanzien van informatiebeveiliging. De BIO biedt een basis om ervoor te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt. Zo kunnen deze bedrijfsonderdelen erop vertrouwen dat gegevens die verstuurd worden naar of worden ontvangen door andere onderdelen van de overheid passend beveiligd zijn. Indien naleving (nog) niet volledig mogelijk is geldt het principe 'comply or explain' wat inhoudt dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om het niet te doen.

De BIO onderscheidt drie basisbeveiligingsniveaus (BBN's): BBN1, BBN2 en BBN3.[16] Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. De ISO 27001 en het VIR bepalen dat het lijnmanagement vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd.

Voor het kiezen van maatregelen gelden met name de BIO (en het VIR-BI) als uitwerking. De BIO bevat een grote hoeveelheid beveiligingsdoelen waarvoor passende maatregelen moeten worden gekozen, samen met een verplichte set aan basismaatregelen. Zoals genoemd, ziet de BIO toe op *informatie* en beveiliging van informatie*systemen*. Het bevat geen verwijzing naar het belang van de gegevens of documenten die door deze systemen gaan.

[15] Zie voor meer informatie: BIO (Baseline Informatiebeveiliging Overheid); Baseline Informatiebeveiliging Overheid; Circulaire toepassen Baseline Informatiebeveiliging Overheid in het digitale verkeer met het Rijk.
[16] Voor meer uitleg over de verschillen tussen de BBNs zie Hoofdstuk 3 van de BIO.

De **Algemene verordening gegevensbescherming** (AVG) en de Uitvoeringswet AVG (UAVG)[17] zien toe op rechtmatig omgaan met *persoonsgegevens*. Zo bepaalt de AVG dat persoonsgegevens alleen verwerkt mogen worden in overeenstemming met de wet, dat het voor betrokkene helder en transparant moet zijn waarom persoonsgegevens verwerkt worden en mogen persoonsgegevens alleen verzameld worden met een gerechtvaardigd doel. De Autoriteit Persoonsgegevens (AP)[18] is de toezichthouder op deze wet en andere wet- en regelgevingen voor de verwerking van persoonsgegevens. De taken en bevoegdheden van de AP als toezichthouder zijn in de AVG en UAVG vastgelegd. Het is verder voor overheidsorganen verplicht om een interne toezichthouder, de functionaris gegevensbescherming (FG)[19], aan te stellen.

2.2. Voor gegevens in basisregistraties

Er bestaan momenteel 10 basisregistraties die samen met enkele stelseldiensten (stelselvoorzieningen en kennisdiensten) het **Stelsel van Basisregistraties**[20] vormen. Een **basisregistratie** is een bij wet geregeld register waarin authentieke gegevens zijn opgenomen.[21] Momenteel zijn er 10 specifieke wetten, één voor elke basisregistratie.[22]

Een basisregistratie is "een door de overheid officieel aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit die door alle overheidsinstellingen verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken".[23] Omdat de gegevens uit het Stelsel van Basisregistraties veel en verplicht gebruikt worden in allerlei (overheids)processen is de kwaliteit van de gegevens belangrijk.[24] Daartoe zijn kwaliteitsnormen opgesteld, bijvoorbeeld met betrekking tot *volledigheid*, *juistheid* en *actualiteit* van gegevens in de basisregistratie.

Binnen het Stelsel van Basisregistraties zijn verschillende stelselrollen actief:[25]

- *Opdrachtgever*: het voor de basisregistratie verantwoordelijke ministerie. Deze is tevens de opdrachtgever voor de 'verstrekker'.
- *Verstrekker*: is verantwoordelijk voor het verstrekken van de gegevens aan afnemers. De verstrekker is ook verantwoordelijk voor het faciliteren van het gebruik (zoals het leveren van kennis en ondersteuning aan afnemers voor het aansluiten op de landelijke voorziening). Een basisregistratie heeft één verstrekker.
- *Toezichthouder*: bij de basisregistraties is de toezichthouder de partij die verantwoordelijk is dat wordt toegezien of de basisregistratie in overeenstemming met eisen, afspraken en wetgeving opereert. Over het algemeen is de opdrachtgever verantwoordelijk voor het toezicht op de naleving van de wettelijke bepalingen die gelden voor die basisregistratie.[26]
- *Bronhouder*: is verantwoordelijk voor het inwinnen en bijhouden van de authentieke en niet-authentieke gegevens in een basisregistratie en voor het borgen van de kwaliteit van die gegevens (onder meer naar aanleiding van ontvangen terugmeldingen). Een basisregistratie heeft één of meer bronhouders.
- *Afnemer* (of gebruiker): is een overheidsorganisatie of private partij die gegevens afneemt van een basisregistratie voor gebruik in de eigen processen. Een organisatie kan zowel verstrekker, bronhouder als afnemer zijn.

[17] Uitvoeringswet Algemene verordening gegevensbescherming (2018).
[18] Zie voor meer informatie: de Autoriteit Persoonsgegevens.
[19] Zie voor meer informatie: Functionaris gegevensbescherming.
[20] Dit zijn: 1) BRP – Basisregistratie personen (bestaat uit ingezetenen en niet-ingezetenen); 2) HR – Handelsregister; 3) BAG – Basisregistratie Adressen en Gebouwen; 4) BRT – Basisregistratie Topografie; 5) BRK – Basisregistratie Kadaster; 6) BRV – Basisregistratie Voertuigen (kentekenregister); 7) BRI – Basisregistratie Inkomen; 8) WOZ – Basisregistratie Waarde Onroerende Zaken; 9) BGT – Basisregistratie Grootschalige Topografie (voorheen GBKN); en 10) BRO – Basisregistratie Ondergrond.
[21] Eis 1: De registratie is bij wet geregeld.
[22] Zie bijvoorbeeld: Wet basisregistratie personen; Wet basisregistratie grootschalige topografie en Wet waardering onroerende zaken.
[23] 10 basisregistraties.
[24] Zie voor meer informatie over de kwaliteitsinformatie per basisregistratie: Kwaliteitsinformatie Stelsel van Basisregistraties 2020.
[25] Rollen Stelsel van basisregistraties - Digitale Overheid
[26] Zie voor een overzicht van de opdrachtgever, de toezichthouder, de verstrekker en de bronhouder(s) per basisregistratie: Rollen.

Complexe maatschappelijke opgaven vragen steeds vaker om samenwerking in ketens en netwerken, waarin gegevens gezamenlijk worden gebruikt. Binnen de Interbestuurlijke Datastrategie (IBDS) is één van de speerpunten om overheidsbrede systeemfuncties te ontwikkelen, waaronder een *federatief datastelsel*, waarmee data beter vindbaar en technisch uitwisselbaar wordt. Het uitgangspunt van het federatief datastelsel is dat data bij de bron wordt bewaard, uitsluitend daar kan worden bevraagd en dat de zorgvuldige omgang met beveiliging en privacy zijn gewaarborgd.[27]

Ten opzichte van het huidige Stelstel van Basisregistraties beoogt het federatief datastelsel de volgende resultaten:

- Een federatie met meer datahouders, een rijker aanbod van stelseldata, meer gebruikers(organisaties) en intensief gebruik van stelseldata, voldoend aan de aansluitvoorwaarden;
- Samenhangende stelselfuncties die zorgen voor de sturing op en de beoogde werking van het federatief datastelsel als vertrouwenssysteem van datagebruik;
- Structurele (door)ontwikkeling van het federatief datastelsel via (maatschappelijke) use cases en een innovatiewerkplaats voor experimenteren en beproeven;
- Structurele governance en financiering voor beheer en doorontwikkeling van het stelsel;
- Overzicht en inzicht in beschikbare data door een flinke uitbreiding van ontsloten open en beschermde data via datacatalogi (IBDS, 2023, p. 15).

2.3. Voor documenten

In verschillende wetten is aangegeven dat overheidsorganen (bestuursorganen) een zorgplicht hebben ten aanzien van documenten. De **Wet open overheid** (Woo)[28] schrijft voor dat een bestuursorgaan er zorg voor draagt dat de documenten die het ontvangt, vervaardigt of anderszins onder zich heeft, zich in goede, geordende en toegankelijke staat bevinden.[29] Er is binnen elk bestuursorgaan dat onder de Woo valt een contactpersoon aangewezen die een soortgelijke functie vervult als de Functionaris Gegevensbescherming van de AVG.

Een soortgelijke zorgplicht staat in de **Archiefwet 2021**: overheidsorganen treffen passende maatregelen om hun documenten in goede, geordende en toegankelijke staat te brengen en te bewaren[30]. De Archiefwet bepaalt welke ambtenaren toezicht houden op de naleving van de wet. Dit toezicht is geregeld per bestuurslaag. Daarnaast houdt de Inspectie Overheidsinformatie en Erfgoed toezicht op het beheer van de archiefbescheiden.

De impact van deze wetten mag niet worden onderschat. Er wordt veel tijd en energie door overheidsorganen besteed aan het ordenen, toegankelijk maken, classificeren en bewaren (of tijdig doen vernietigen – zie hierna). Dit is volstrekt begrijpelijk vanuit een praktijk waarin informatie werd vastgelegd in fysieke documenten in fysieke dossiers en fysieke archiefkasten; om dat te kunnen ontsluiten is een systematiek nodig die op elk document, elk dossier en elke kast wordt toegepast. En wat leidt tot kilometers fysiek archief, wat ontegenzeggelijk tegen grenzen op loopt.

De basis voor informatiebeveiliging van alle informatieprocessen bij de Rijksdienst is geregeld in het **Voorschrift Informatiebeveiliging Rijksdienst** (VIR). Op de beveiliging van bijzondere informatie zijn de bepalingen van het **Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013** (VIRBI 2013)[31] als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst (BIR 2007)[32] en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013)[33] van

[27] Voor meer informatie zie: Van datastrategie naar datastelsel.
[28] Wet open overheid (2022).
[29] Wet open overheid (2022) Artikel 2.4. Zorgplicht en openbaarmaking.
[30] Voorstel van Wet tot intrekking van de Archiefwet 1995 en vervanging door de Archiefwet 2021 (Archiefwet 2021) Artikel 3.1.
[31] VIRBI (2013).
[32] Besluit voorschrift informatiebeveiliging rijksdienst (2007).
[33] Beveiligingsvoorschrift Rijksdienst 2013.

toepassing. Nederland kent vier rubriceringsniveaus op bijzondere informatie: Staatgeheim ZEER GEHEIM, Staatgeheim GEHEIM, Staatsgeheim CONFIDENTIEEL, Departementaal VERTROUWELIJK. Hierbij is het de *opsteller* van de informatie die een voorstel tot rubricering aanbrengt op de informatie waarna de *vaststeller* van de inhoud van de informatie de rubricering vaststelt. Bijzondere informatie wordt zodanig beveiligd dat alleen geautoriseerde personen de informatie kunnen behandelen of inzien voor zover dit noodzakelijk is voor hun taak en dat het onrechtmatig raadplegen van de informatie wordt gedetecteerd. Over toezicht is in het VIRBI 2013 opgenomen dat het ministerie toezicht uitoefent op de beveiliging van het door het ministerie gecreëerde bijzondere informatie. Het toezicht is per departement geregeld, wat volgens respondenten het risico vergroot dat er verschillen in toezicht zijn en daarmee ook verschillen in de wijze van naleving ontstaan. Inbreuk op gerubriceerde informatie moet direct gemeld worden bij de Beveiligingsambtenaar (BVA) van het departement waarna deze persoon onmiddellijk (nood)maatregelen treft om verdere inbreuk te voorkomen. [34]

Met het VIRBI 2013 is binnen de Rijksdienst geregeld hoe om te gaan met bijzondere informatie, maar het VIRBI biedt geen kader voor de medeoverheden. Het is de wens van het ministerie van BZK om de wetgeving en voorschriften voor bijzondere informatie te harmoniseren.

2.4. Voor digitale processen: NIS en straks NIS2

Als gevolg van de herziening van **de Netwerk- en informatiebeveiligingsrichtlijn** (NIS2) krijgen veel meer sectoren en organisaties binnen de EU te maken met wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen. Dit betekent ook dat de Nederlandse wettelijke vertaling van de NIS, de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni), herzien zal worden. In deze wet staan nu maatregelen om de digitale weerbaarheid te vergroten.[35] De Wbni geldt naast digitale aanbieders ook voor digitale dienstverleners. Digitale dienstverleners kunnen met behulp van de Wbni *self-assessment* bepalen of de Wbni op hun organisatie van toepassing is. Zij kunnen hiermee ook bepalen of de genomen maatregelen aansluiten bij de doelstellingen van de Wbni. Daarnaast hebben organisaties in vitale sectoren en digitale dienstverleners een meldplicht van incidenten op netwerk- en informatiesystemen en een zorgplicht. Indien een incident met aanzienlijke gevolgen zich voordoet, dan moet dit gemeld worden bij Rijksinspectie Digitale Infrastructuur (RDI) en bij een Computer Security Incident Response Team (CSIRT). De RDI is de toezichthouder op de naleving van de Wbni voor de energiesector, voor digitale dienstverleners en de digitale infrastructuur. Voor aanbieders van essentiële diensten is het Nationaal Cybersecurity Centrum (NCSC) de aangewezen CSIRT. Het ministerie van BZK is vanuit de NIS2-richtlijn verantwoordelijk voor het organiseren van toezicht op de sector overheid.

De NIS2 betreft reeds gereguleerde sectoren in het bedrijfsleven, de overheid en sectoren die nu nog niet onder de NIS1 vallen zoals afvalwater, ruimtevaart, de centrale overheid en levensmiddelen. Deze organisaties krijgen een formele zorgplicht waardoor ze proportionele maatregelen moeten nemen.[36] De NIS2 schrijft niet voor hoe de gevoeligste informatie moet worden beschermd wanneer samengewerkt wordt in ketens en netwerken van organisaties.

[34] VIRBI (2013) - Artikel 8. Compromittering van bijzondere informatie.
[35] Zie voor meer informatie over de Wbni: Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners.
[36] De staatssecretaris van BZK heeft op 5 april tijdens het Commissiedebat Informatiebeveiliging bij de overheid officieel kenbaar gemaakt dat medeoverheden onder de NIS2-richtlijn zullen vallen onder *belangrijke entiteiten*.

2.5. Tussenconclusie

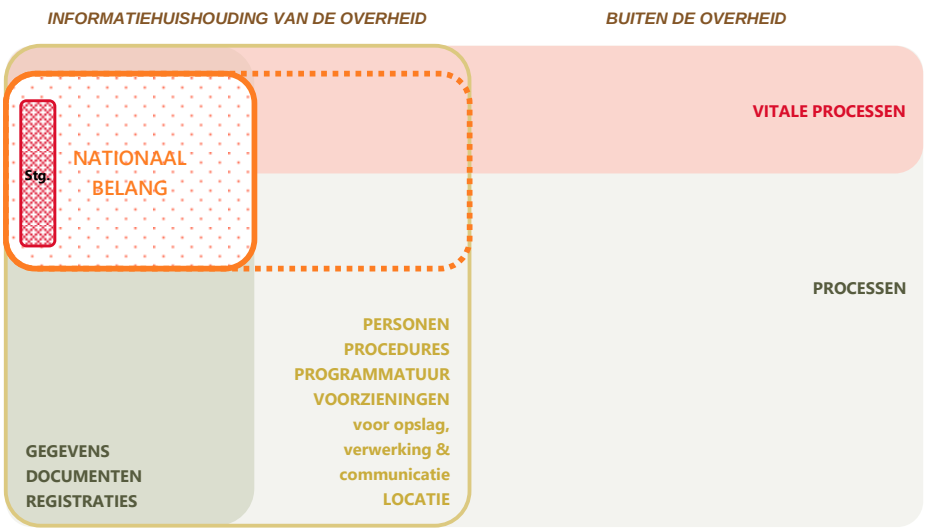
Voor het beschermen van gegevens, documenten, registraties, informatie, processen en systemen bestaan al diverse wettelijke kaders. Deze vullen elkaar soms aan, maar zijn afhankelijk van de risico-inschatting van de houder en de daaropvolgende keuzes of en hoe bescherming wordt ingevuld. Daarnaast is het toezicht op documenten momenteel niet volstrekt onafhankelijk en mogelijk evenmin uniform.

Er kan bovendien ruwweg een tweedeling gemaakt worden tussen enerzijds gegevens, documenten en registraties en anderzijds informatie, processen en systemen. Gegevens, documenten en registraties hebben veelal een onveranderlijk karakter (of zouden dat moeten hebben – een reden om de integriteit ervan te beschermen) terwijl informatie, processen en systemen zich baseren op deze gegevens, documenten en registraties, er veranderingen in aanbrengen en bijdragen aan het produceren van nieuwe gegevens, documenten en registraties. Bovendien maakt nieuwe technologie mogelijk dat gegevens, documenten en registraties steeds opnieuw, ook gelijktijdig, (her)gebruikt kunnen worden door heel diverse en over tijd veranderende processen en systemen.

De staatssecretaris Koninkrijksrelaties en Digitalisering wil informatieveiligheid bij de overheid een wettelijke basis geven via een zorgplicht waaraan nadere regels kunnen worden gesteld, zoals de BIO[37]. Door het wettelijk verplichten van de BIO is de vrijblijvendheid voorbij. Door op één plaats een algemene zorgplicht voor informatieveiligheid bij de overheid te regelen wordt een vereenvoudiging van regels binnen de overheid bereikt. Daardoor komt de focus meer te liggen op het feitelijk beveiligen in plaats van administratief beveiligen. Bij een dergelijke zorgplicht past ook aparte aandacht voor de belangrijkste processen. Dat zijn niet alleen de vitale overheidsprocessen, dat kunnen ook andere 'kroonjuwelen' zijn. Voor deze 'kroonjuwelen' wil de staatssecretaris, samen met vitale overheidsprocessen en processen waar staatsgeheimen in rondgaan, een hogere mate van zorgvuldigheid bereiken. Als duidelijk is wat deze (digitale) 'kroonjuwelen' zijn, die kunnen worden aangemerkt als 'van Nationaal Belang', dan kunnen aan organisaties, systemen en processen die gebruikmaken van die 'kroonjuwelen' eisen worden gesteld ten aanzien van beveiliging van deze digitale kroonjuwelen.

In Figuur 2 hieronder is de reikwijdte weergegeven van wat als 'Nationaal Belang' wordt aangeduid in dit onderzoek: het betreft gegevens, documenten en registraties binnen de overheid, waarbinnen in elk geval ook alle gerubriceerde gegevens, documenten en registraties vallen. Het Nationaal Belang zal deels overlappen met (gegevens, documenten en registraties in) vitale overheidsprocessen, maar in elk geval zullen ook gegevens, documenten en registraties in niet-vitale overheidsprocessen tot Nationaal Belang kunnen behoren. De verwerking van gegevens, documenten en registraties van Nationaal Belang dient vanwege de hoogste mate van vertrouwelijkheid, beschikbaarheid en/of integriteit specifieke (extra) eisen te stellen aan personen, procedures, systemen, (fysieke) locaties voor opslag, etc.

[37] Zie: Brief betreffende Generiek kader voor vitale digitale processen van de overheid, https://www.tweedekamer.nl/downloads/document?id=2022D38545.



Figuur 2: Reikwijdte van Nationale Belangen

Dit leidt ertoe dat het feitelijk het meest voor de hand ligt om bescherming van Nationale Belangen te starten bij het beschermen van authentieke voor de Nederlandse maatschappij belangwekkende gegevens, documenten en registraties, om vervolgens eisen te stellen aan processen en systemen (en aan de mensen en organisaties die daarmee werken en de fysieke locaties waar ingrijpen op systemen waarop verwerking of opslag plaatsvindt). De redenering is: betreft het gegevens, documenten of registraties van Nationaal Belang? Dan dienen processen, systemen, etc. minimaal ook te voldoen aan daarbij passende beveiligingseisen.

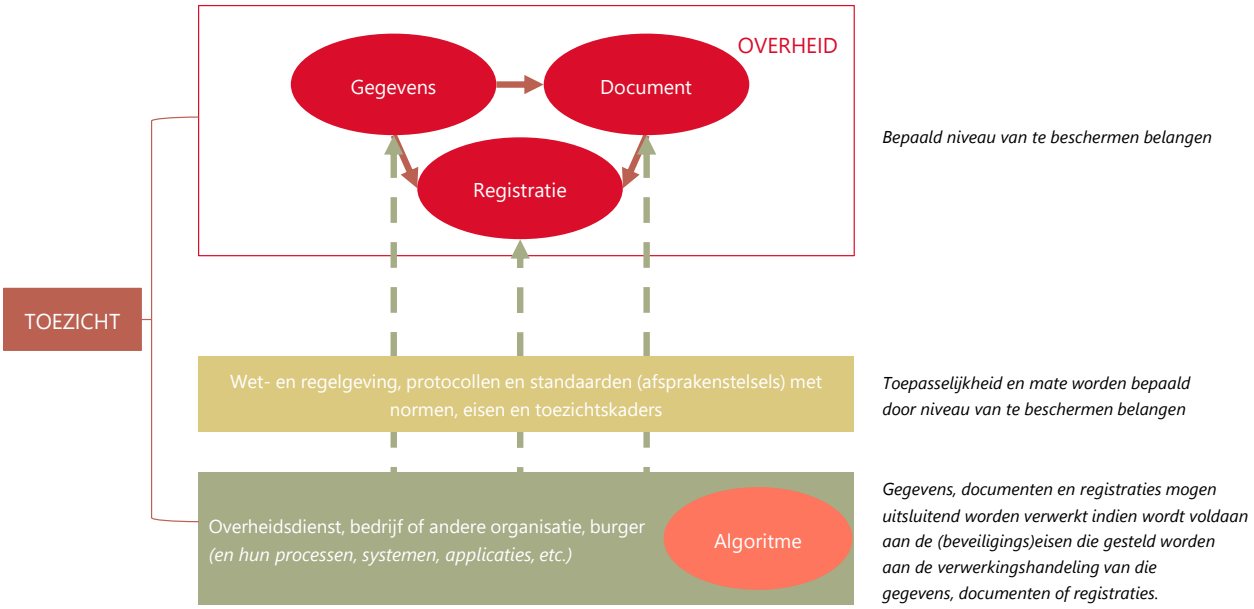
Het volgende hoofdstuk richt zich op de wijze waarop kan worden afgewogen welke gegevens, documenten en registraties van groter belang zijn dan andere en welke zelfs van Nationaal Belang zijn.

3. Belangenafweging

Er bestaat momenteel geen generieke methode voor het afwegen van belangen. Dit hoofdstuk richt zich op de wijze waarop kan worden afgewogen welke gegevens, documenten en registraties van groter belang zijn dan andere en welke zelfs van Nationaal Belang zijn.

3.1. Redeneerlijn voor Nationale Belangen

In Figuur 3 staat de in dit rapport gevolgde redeneerlijn voor Nationale Belangen. De overheid (Rijksoverheid, maar ook andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties) genereert, verzamelt en beheert gegevens en documenten. Soms worden gegevens verwerkt tot een document, vaak worden gegevens en documenten bijeengebracht in registraties.



Figuur 3: Redeneerlijn voor Nationale Belangen

Andere onderdelen van de overheid, maar ook bedrijven, niet-overheidsorganisaties en burgers (en hun processen, systemen en applicaties) willen gebruik maken van deze gegevens, documenten en registraties. Op basis van diverse wet- en regelgeving, protocollen, standaarden, etc. worden gegevens gedeeld (uitgewisseld, geraadpleegd) met deze andere onderdelen van de overheid, maar ook bedrijven, niet-overheidsorganisaties en burgers, *voor zover deze daartoe gerechtigd zijn*. Deze uitwisseling geschiedt in aanzienlijk mate door voorzieningen die identificaties/authenticatie en uitwisseling/raadpleging mogelijk maken.

De mate van belang van de gegevens, documenten en registraties bepaalt welke eisen worden gesteld aan beveiliging:

- integriteit (is de informatie juist en zonder fouten?);
- beschikbaarheid (is de informatie beschikbaar op het moment dat die nodig is?);
- en de vertrouwelijkheid of exclusiviteit (is de informatie alleen toegankelijk voor gerechtigde personen?).

Hoe groter het belang, hoe hoger de eisen aan beveiliging. En dus hoe hoger de eisen aan systemen en processen ten behoeve van opslag, verwerking en uitwisseling van gegevens. Hoe hoger de eisen aan de organisaties en personen die deze gegevens verwerken (zelfs ook al: raadplegen).

Voor een beperkte categorie gegevens, documenten en registraties geldt dat hun belang niet alleen dat van de individuele overheidsorganisatie overstijgt, maar dat deze zelfs het belang van de gehele overheid overstijgt en van Nationaal Belang zijn. Denk daarbij aan gegevens waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries – de definitie van bijzondere informatie in het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).[38] Maar ook officieel een aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit, die door alle overheidsinstellingen verplicht en zonder nader onderzoek worden gebruikt bij de uitvoering van publiekrechtelijke taken – de definitie van een basisregistratie.[39] Maar welke gegevens, documenten en registraties kunnen naast bijzondere informatie en basisregistraties mogelijk nog meer worden aangemerkt als van Nationaal Belang?

Als onderdeel van het onderzoek welke criteria leiden tot Nationaal Belang, hebben wij onderzocht met welke afwegingen van belangen, gegevens, documenten en registraties kunnen worden aangemerkt als *van Nationaal Belang*. Wij hebben gesproken met 30 respondenten in 24 interviews. In deze interviews is onder andere aan de respondenten gevraagd of de organisatie waar zij werkzaam zijn een belangenafweging maakt voor zaken die in hun organisatie belangrijk zijn en aan de hand van welke methodiek deze belangenafweging plaatsvindt, wat volgens hen aangemerkt moet worden als zijnde Nationaal Belang, of zij de noodzaak begrijpen van deze 'extra' classificatie en hoe de huidige richtlijnen en kaders worden ervaren.

Respondenten gaven in algemene zin aan dat het maken van een belangenafweging, het selecteren van datgene binnen een organisatie dat dermate belangrijk is dat er mogelijk extra toezicht en maatregelen moeten worden ingericht, voor een deel gebeurt op basis van 'gezond verstand': "belangrijk zijn die zaken die de organisatie aanmerkt als belangrijk". Een relevante vraag die hierbij - impliciet of expliciet - wordt gesteld is vaak: 'wat gebeurt er met het primaire proces van de organisatie, hetgeen waarvoor de organisatie is opgericht of in stand wordt gehouden, als dit onderdeel uitvalt?'. Respondenten gaven aan dat er momenteel geen algemene methodiek noch een generiek proces is binnen de Rijksoverheid voor het maken van een belangenafweging. Zij geven aan wat zorgen te hebben over de verschillende interpretaties van bestaande (wettelijke) kaders en de mate van volwassenheid van sommige lagen. Wel werd aangegeven dat er op deelgebieden dergelijke belangenafwegingen worden gemaakt, zoals voor gegevens en systemen (ten behoeve van autorisaties), documenten (archivering en rubricering) en systemen en processen (voor beveiliging). Hieruit zijn aanknopingspunten te identificeren die mogelijk bruikbaar zijn voor het opstellen van een generiek proces voor het maken van een belangenafweging om te komen tot het kunnen aanwijzen van gegevens, documenten en registraties die van Nationaal Belang zijn.

In dit hoofdstuk worden bestaande werkwijzen en mogelijke aangrijpingspunten verder uitgelicht met als doel een antwoord te formuleren op de deelvragen:

- Welke eenvoudige en onbetwiste criteria leiden tot een nationaal belang?
- Welke concrete eisen moeten aan risicomanagement gesteld worden? (Het gaat hier specifiek om risicomanagement voor Nationale Belangen om te identificeren waar welke risico's zitten als een organisatie Nationale Belangen verwerkt).

[38] Zie: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).
[39] Zie: 10 basisregistraties.

Uit de interviews en documentenstudie volgen aanknopingspunten voor mogelijke criteria voor een generiek proces van belangenafweging voor Nationaal Belang. Wij gaan hier telkens uit van de gegevens, documenten en registraties die aangemerkt zijn (of zouden moeten worden) als kroonjuwelen (van Nationaal Belang), ongeacht in welk proces deze zitten. Onderstaande voorbeelden van bestaande werkwijzen laten zien hoe kan worden gekomen tot een gedegen belangenafweging.

3.2. Afwegen van belangen bij archiefstukken

Bij het bepalen van een rubricering is al een inschatting gemaakt van het belang van een document. Bij het bij wet instellen van een registratie is het belang van het voeren van een registratie al vastgesteld. Voor sommige registraties (niet ingesteld bij wet), gegevensgegevens en (niet gerubriceerde) documenten is het goed alsnog een belangenafweging te maken. Bij de keuze voor bewaren of vernietigen van archiefbescheiden kan een belangenafweging niet plaatsvinden op gegevenselement of documentniveau. Daarom is door de overheid gekozen om waardering en selectie langs de lijnen van de feitelijke informatiestructuren, de werkprocessen, al dan niet in combinatie met andere gebruikte structurerings- of metadaterings-mechanismen te organiseren. Van deze afzonderlijke informatiestructuren wordt vervolgens afgewogen of de archiefbescheiden die hierin ontstaan dienen te worden bewaard of vernietigd.

De *Handreiking waardering en selectie. Belangen in balans*[40] van het Nationaal Archief uit maart 2015 geeft richtlijnen voor waardering en selectie van informatie[41]: het toekennen van waarde aan informatie en vervolgens kiezen: wat mag blijven en wat wordt vernietigd? Waarderen is volgens de *Handreiking* het toekennen van waarde: "Waardering van archiefbescheiden gebeurt voor verschillende doeleinden. Bijvoorbeeld om aan te geven welke informatie gepubliceerd kan worden of juist voorlopig niet in de openbaarheid mag komen of *welke informatie optimaal beveiligd dient te worden*. Een ander oogmerk van waarderen is bepalen welke informatie hoe lang bewaard dient te worden. Op deze laatste categorie richt deze handreiking zich. Vaak hangen de verschillende vormen van waarderen van informatie samen. Om die reden is het verstandig – waar mogelijk – de verschillende waarderingsvormen in samenhang toe te passen."[42] De belangrijkste afwegingsfactoren bij waardering worden bepaald door *het specifieke bedrijfsbelang* (inclusief juridisch en financieel belang), het *politieke belang* (inclusief verantwoordingsbelang) en *het maatschappelijk belang* (inclusief het belang van de recht- en bewijszoekende burger, het historisch belang en het erfgoedbelang).

Genoemde belangen worden in de *Handreiking* geoperationaliseerd aan de hand van onderstaande vragen:

- Hoe lang is informatie die is vastgelegd in archiefbescheiden voor het overheidsorgaan (of voor andere organen) nodig om het werk te kunnen uitvoeren? Deze vraag wordt beantwoord aan de hand van de risicoanalyse.
- Welke informatie heeft de organisatie nodig om zich te kunnen verantwoorden: politiek, maatschappelijk (jegens de recht- en bewijszoekende burger), financieel en juridisch? En hoe lang is die verantwoordingsinformatie nodig? Ook deze vragen worden beantwoord aan de hand van de risicoanalyse.
- Van welke informatie is te voorzien dat deze van bijzondere emotionele of symbolische betekenis is voor groepen in de samenleving? Deze vraag wordt beantwoord aan de hand van de hotspot-monitor.
- Welke informatie is nodig om de geschiedenis van het handelen van een organisatie (zowel van zichzelf als ten opzichte van andere organisaties en de samenleving) te kunnen reconstrueren? Deze vraag wordt beantwoord aan de hand van de systeemanalyse.

[40] Handreiking waardering en selectie.
[41] Informatie staat in gegevens, documenten of hele registraties met gegevens en/of documenten. De Archiefwet 1995 spreekt daarom van Archiefbescheiden: Informatie die in de context van het functioneel handelen van een overheidsorgaan wordt gemaakt of ontvangen.
[42] Uit 'Belangen in Balans: Handreiking voor waardering en selectie van archiefbescheiden in de digitale tijd' (2015). Nationaal Archief: Ministerie van Onderwijs, Cultuur en Wetenschap, p. 27.

Met name de hierboven genoemde *risicoanalyse* en *systeemanalyse* lijken ook relevant voor het bepalen van wat de belangrijkste processen, systemen en/of informatie zijn. "Het doel van een risicoanalyse is … vooral ook om *het belang vast te stellen van een bedrijfsproces en de informatie die daarin omgaat*."[43] In de risicoanalyse wordt vastgesteld welke soorten *risico's er zijn voor de organisatie ten aanzien van het niet tijdig en volledig beschikbaar hebben van informatie*. Op basis hiervan kunnen verschillende risiconiveaus worden onderscheiden en risicoprofielen worden bepaald. Risicoprofielen worden vastgesteld door het topmanagement. Sommige organisaties hebben al vastgestelde risicoprofielen waarmee bepaald kan worden welke werkprocessen als hoog-risicoprocessen worden beschouwd. Ook is in deze risicoanalyse van belang om vast te stellen of er bijzondere wet- en regelgeving is waardoor bepaalde gegevens verplicht vernietigd moeten worden of voor een bepaalde periode bewaard moeten blijven (denk aan sectorale wet- en regelgeving, EU-wetgeving en internationale verdragen). Deze risicoanalyse lijkt – indien niet louter gericht op selectie van archiefbescheiden - ook uitstekend geschikt voor het bepalen van Nationale Belangen.

De *systeemanalyse* "brengt op organisatieniveau de structuren (relaties tussen actoren, functies en archiefbescheiden) in kaart om de wezenlijke informatie te identificeren die nodig is om de activiteiten van een organisatie te kunnen reconstrueren. Een functionele analyse vormt de basis van de systeemanalyse. Vervolgens worden de belangrijkste informatieknooppunten binnen de organisatie geïdentificeerd."[44] De systeemanalyse begint met het analyseren van de missie, doelstellingen en kerntaken van de organisatie. Die geven meestal in kernachtige bewoordingen weer waartoe de organisatie in het leven is geroepen. De systeemanalyse concentreert zich vanuit de institutionele invalshoek op de organisatiestructuur en de taakuitvoering. Dat betekent dat de onderdelen waaruit de organisatie is opgebouwd in kaart gebracht worden. Ook wordt vastgesteld of er werkprocessen zijn die door de organisatie zelf *als de meest cruciale* worden beschouwd (hetgeen (tijdelijk) politiek bepaald kan zijn). In de systeemanalyse wordt verder ook in kaart gebracht welke nationale (basis)registraties door de organisatie worden bijgehouden en voor welke (basis)registraties de organisatie verantwoordelijk is. Nationale (basis)registraties die cruciale informatie bevatten over personen, organisaties, gebouwen, geografie en economie komen in aanmerking voor blijvende bewaring. Ze worden beschouwd als belangrijke informatieknooppunten. In deze (basis)registraties zijn de opbouw en ontwikkeling van de Nederlandse samenleving en het Nederlandse grondgebied vastgelegd. Ook deze systeemanalyse biedt bouwstenen voor het bepalen van Nationale Belangen.

Het kunnen uitvoeren van de bovenstaande risicoanalyse en systeemanalyse veronderstelt dat er in de meest eenvoudige vorm een overzicht is van de werkzaamheden die de organisatie uitvoert, met per werkproces aangegeven de (categorieën van) informatie[45] die daarbij worden gegenereerd. Daarbij wordt verwezen naar een citaat van W.E. Deming: "*If you can't describe what you are doing as a process, you don't know what you're doing*"[46]: het beginpunt van effectief informatiebeheer is niet de informatie, maar het werkproces waarbinnen informatie wordt gegenereerd. Kennis van de werkprocessen die worden uitgevoerd, vormt de basis voor alle vormen van informatiebeheer.

De methode om waarde aan informatie toe te kennen die wordt gehanteerd door het Nationaal Archief zou kunnen worden gebruikt om niet alleen te bepalen welke informatie mag blijven en welke informatie moet worden vernietigd, maar ook om vast te stellen welke informatie van grotere waarde is dan andere en welke informatie zelfs zo'n grote waarde heeft – de belangrijkste informatie – dat deze van Nationaal Belang is. De *Handreiking waardering en selectie* richt zich specifiek op de departementen, inclusief diensten en agentschappen, maar volgens de geraadpleegde versie zou in 2015 de scope worden uitgebreid naar de gehele Rijksoverheid (inclusief de zelfstandige bestuursorganen) en

[43] Uit 'Belangen in Balans: Handreiking voor waardering en selectie van archiefbescheiden in de digitale tijd' (2015). Nationaal Archief: Ministerie van Onderwijs, Cultuur en Wetenschap, p. 15.
[44] Ibidem, p. 18.
[45] De *Handreiking* spreekt hier uiteraard van archiefbescheiden.
[46] Uit 'Belangen in Balans: Handreiking voor waardering en selectie van archiefbescheiden in de digitale tijd' (2015). *Nationaal Archief: Ministerie van Onderwijs, Cultuur en Wetenschap*, p. 37.

naar de andere overheden – die laatste uitbreiding in nauw overleg met de koepels VNG, IPO en UvW. Ook waardering (en selectie) in ketenprocessen zou later nog speciale aandacht krijgen.

Deze systematiek zou wel tot minder gewenste uitkomsten kunnen leiden als het gaat om gegevens, documenten en registraties die op één plek, bij de bron, worden opgeslagen en beheerd, maar door diverse organisaties in ketens en netwerken worden verwerkt – een ontwikkeling die hiervoor al is geschetst. Een afweging van en door de organisatie die de houder is zou wellicht onvoldoende rekening kunnen houden met het belang van die gegevens, documenten en registraties in de processen van derden[47].

Dit wordt enigszins gecompenseerd doordat selectielijsten moeten worden voorbereid door een Strategisch Informatie Overleg (SIO). De specifieke invulling van dit overleg verschilt per type zorgdrager (departementen, ZBO's en PBO's en decentrale overheden), maar bij de departementen nemen de Chief Information Officer (CIO) en de algemene rijksarchivaris structureel deel aan het SIO. Bij de behandeling van een ontwerpselectielijst wordt ook een externe deskundige betrokken. Deze persoon die betrokken wordt, moet deskundig zijn op het terrein van de relatie tussen burger en overheid en de betekenis van overheidsinformatie voor deze relatie. Daarnaast wordt gesteld dat een deskundige bij voorkeur kennis heeft van de beleidsterreinen waarop de indienende zorgdrager actief is. Een voorbereiding in dit gremium kan bijdragen aan een brede(re) blik op de waarde van gegevens, documenten en registraties, niet alleen voor de zorgdrager zelf. Juist het expliciet afwegen van dit belang voor processen buiten de eigen organisatie en voor andere organisaties in ketens en netwerken is een belangrijk element in een afweging in het kader van Nationale Belangen.

Ook nog relevant in het kader van dit onderzoek is dat de uiteindelijke (archief)selectielijsten, op basis van de weging van belangen (risicoanalyse, systeemanalyse en hotspot-monitor) formeel worden vastgesteld:

- Archiefbescheiden van de Eerste en de Tweede Kamer der Staten-Generaal, de andere Hoge Colleges van Staat en het Kabinet van de Koning: bij koninklijk besluit, op voordracht van Onze minister, in overeenstemming met het betrokken overheidsorgaan;
- Archiefbescheiden van de ministeries: door Onze minister en Onze minister wie het mede aangaat;
- Archiefbescheiden van andere overheidsorganen: door Onze minister.

Deze vaststelling geschiedt dus op een centraal niveau.

Toezicht op een juiste en tijdige uitvoering van de archiefselectie wordt uitgevoerd door één toezichthouder voor de gehele Rijksoverheid: de Inspectie Overheidsinformatie en Erfgoed. De provincies zien op grond van de Gemeentewet toe op de uitvoering van de Archiefwet. Vanuit dit interbestuurlijk toezicht beoordelen de provincies de situatie bij gemeenten en waterschappen.

[47] "Uitgangspunt is de verantwoordelijkheid die de zorgdager heeft voor uitvoering van de werkzaamheden waar de organisatie voor in het leven is geroepen. Hierbij hoort uitdrukkelijk de verplichting om zich te kunnen verantwoorden en de rechten bewijszoekende burger te dienen. Het primaire object van waardering bij de risicoanalyse zijn de activiteiten die de zorgdrager uitvoert (werkprocessen)." Niet expliciet wordt genoemd het belang van gegevens, documenten of registraties voor de activiteiten die derden uitvoeren. Zie: 'Belangen in Balans: Handreiking voor waardering en selectie van archiefbescheiden in de digitale tijd' (2015). Nationaal Archief: Ministerie van Onderwijs, Cultuur en Wetenschap, p. 13.

3.3. Te Beschermen Belangen in het BVA-stelsel

Ieder departement heeft een beveiligingsambtenaar (BVA) die verantwoordelijk is voor de *integrale beveiliging*: "het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen voor de beveiliging van de Te Beschermen Belangen op basis van risicomanagement".[48] *Te Beschermen Belangen* (TBB) zijn volgens het Besluit BVA-stelsel Rijksdienst "Staatsbelangen die beveiligd moeten worden om de werking van de Rijksoverheid te garanderen".[49] TBB's zijn gedefinieerd als "personen, informatie, informatiesystemen, materieel, goederen, imago en objecten, waarbij in geval van compromitteren of de mogelijkheid van compromitteren, nadelige gevolgen, of een risico daarop, kan ontstaan voor de vertrouwelijkheid, beschikbaarheid en integriteit van de primaire processen van de rijksoverheid, delen daarvan of voor andere belangen van de Staat, van zijn bondgenoten of van één of meer ministeries".[50]

Risicomanagement is in dit Besluit gedefinieerd als het "inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes".[51] Het TBB-overzicht kent per departement één eigenaar en één administratief beheerder.[52] Minimaal één keer per jaar dient op last van de eigenaar van de TBB-basisadministratie een complete validatie van de TBB-lijst plaats te vinden door de TBB-eigenaren.[53]

"Om de TBB op het juiste niveau te beschermen is het noodzakelijk te komen tot een afgewogen geheel aan organisatorische, bouwkundige, elektronische en informatie-technische beveiligingsmaatregelen. Voor het vaststellen van de noodzakelijke beveiligingsmaatregelen is het van belang om een beeld te hebben van de dreiging waaraan een TBB is blootgesteld en de impact van onverhoopt optredende schade aan een TBB. *Verder dient duidelijk te zijn wat het belang is van de betreffende TBB voor het ongestoord functioneren van het departement en/of Rijksoverheid*. […] Op basis van *impactcriteria* worden TBB ingedeeld in vier categorieën. De categorale indeling geldt als hulpmiddel voor de prioritering bij de toewijzing van passende (beveiligings)middelen en helpt bij het maken van keuzes voor de inzet van de noodzakelijke beveiligingsmaatregelen (risicomanagement) ter bescherming van de TBB" (Leidraad: Te Beschermen Belangen, 2015, p. 3).

De *Leidraad: Te Beschermen Belangen* schrijft voor dat een compleet en actueel inzicht in (statische) TBB en/of locaties waar zich TBB bevinden (zogenaamde risicoplaatsen) het startpunt vormt voor de selectie en implementatie van beveiligingsmaatregelen. Hier wordt gesteld dat het beginpunt van een goede beveiliging is: weten wat beveiligd moet worden.[54] Integrale beveiliging biedt ondersteuning en borgt de continuïteit en betrouwbaarheid van de bedrijfsprocessen van het departement. Dit maakt integrale beveiliging geen doel op zich, maar het beschermt tegen onder meer dreigingen die kunnen optreden als gevolg van opzettelijk menselijk handelen en onopzettelijk menselijk falen. Het integrale karakter van de beveiliging komt tot uiting in de samenhang tussen de maatregelen in de verschillende onderdelen van het primaire proces en de – daaraan ondersteunende – bedrijfsvoering en -middelen.[55]

[48] Besluit BVA-stelsel Rijksdienst, 2021, p. 1.
[49] Uit Leidraad: Te Beschermen Belangen, 2015 p. 3.
[50] Ibidem.
[51] Ibidem.
[52] Leidraad: Te Beschermen Belangen, 2015, p. 7.
[53] Ibidem.
[54] Leidraad: Te Beschermen Belangen, 2015, p. 7.
[55] Besluit BVA-stelsel Rijksdienst, 2021, p. 7.

Om te komen tot een categorale indeling van de TBB dient onder andere rekening te worden gehouden met:

a. Het rubriceringsniveau van de informatie of van het informatiesysteem;
b. De kwetsbaarheid, vervangbaarheid (schaarste) en reparatiemogelijkheden van het materieel en/of object in geval van (moedwillige) vernieling;
c. De hoogte van de vervangingskosten van het materieel en/of object;
d. De (imago)schade voor een (bewinds)persoon, een departement, of in extreme gevallen voor de gehele Rijksoverheid in geval een TBB is gecompromitteerd.[56]

Bij het bepalen van TBB's worden personen, informatie, informatiesystemen, materieel, goederen, imago en objecten geïdentificeerd en geclassificeerd. *De mate van vitaliteit van de belangen van de Staat of een belang van één of meerdere departementen is bepalend voor de TBB-categorie*. Op basis van de *impactcriteria* (zie Tabel 1[57]) worden TBB ingedeeld in vier categorieën:[58]

- TBB 1: Impact Zeer hoog (gelijk aan Stg. Zeer geheim);
- TBB 2: Impact Hoog (gelijk aan Stg. Geheim);
- TBB 3: Midden (gelijk aan Stg. Confidentieel);
- TBB 4: Laag (gelijk aan Dep. Vertrouwelijk).

Politieke schade	Imago schade	Diplomatieke schade	Schade vitale processen samenleving	Letsel schade	Betrouwbaar-heidseisen IT-systemen (quickscan BIR)	VIR-BI	Inter-natio-naal (NAVO /EU)	Financiële schade economie/ Staat (€)	Financiële schade door misbruik bedrijfsinformatie (€)	TBB
Geen	Geen	Geen	Geen invloed	Geen	ZL,ZL,ZL			≤ 50 mln.	≤ 1 mln.	
Politieke schade voor bewinds-persoon	Verlies aan publiek respect	Te herstellen door ambtelijke opschaling	Verlies van zekerheid van continuïteit	Individuele gewonde	t/m H,H,H	Ongerubr. met merking; Dep. V	NATO-RESTR EU-RESTR	> 50 mln.	> 1 mln.	4
Aftreden bewinds-persoon	Publieke veront-waardiging	Te herstellen door politieke opschaling	Tijdelijk verlies van continuïteit	Individuele dode, zeer ernstig gewond	Eén van de aspecten ZH	Stg. CONFI	NATO - CONFI EU-CONFI	> 500 mln.	> 5 mln.	3
Aftreden kabinet	Verlies aan vertrouwen	Externe bemiddeling noodzakelijk	Langdurig verlies van continuïteit	Meerdere doden, ernstig gewonden	Alle aspecten ZH	Stg. GEHEIM	NATO SECRET EU-SECRET	> 5 mld.	> 500 mln.	2
Parlemen-taire crisis	Structureel verlies aan vertrouwen	Lange termijn schade ten opzichte van bondgenoten; oorlog	Blijvende uitval van processen	Groepen Doden		Stg. ZEER GEHEIM	COSMIC TOP SECRET EU-TOP SECRET	> 50 mld.	> 5 mld.	1

Tabel 1: Impacttabel TBB

Bij TBB1 en TBB2 is sprake van (zeer) ernstige *schade* indien kennisname door niet-gerechtigden, aantasting of verlies kan leiden tot een dusdanig nadelig effect of het functioneren van de Rijksoverheid dat tenietdoen van dat effect niet of slechts na zeer grote investeringen in tijd, arbeid en kapitaal mogelijk is. Of indien kennisname door niet-geautoriseerde zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of/en zijn bondgenoten. De mate van *belangen* en de *impact* die deze hebben bij eventuele uitval of misbruik, geven aan dat deze worden gezien als van 'het hoogste belang' en lijkt daarom van hetzelfde belang als Nationale Belangen.

[56] Leidraad: Te Beschermen Belangen, 2015, p. 4.
[57] Leidraad: Te Beschermen Belangen, 2015, p. 9.
[58] Ibidem.

De classificatie van *Te Beschermen Belangen* is heel goed toepasbaar voor classificatie van gegevens, documenten en registraties die kunnen worden aangemerkt als van Nationaal Belang. Respondenten benoemen dat deze methode de mogelijkheid biedt om na te gaan hoe kritiek een systeem is door het 'af te pellen': wat gebeurt er als mijn primaire proces (voor een periode) wegvalt? Zij benoemen dat de bestaande leidraad deze methode goed beschrijft en voldoende handvatten biedt. Maar zij wijzen erop dat ook in deze leidraad de afweging aan het eigen departement is en dat niet staat beschreven hoe om te gaan met TBB – bijvoorbeeld gerubriceerde documenten - die worden gedeeld met andere overheden of door ketens of netwerken gaan. Zij benadrukken dat ook hier de kans bestaat dat door verschillen in interpretaties en weging er verschillende uitkomsten mogelijk zijn tussen departementen, wat voor gegevens van Nationaal Belang onwenselijk is.

3.4. Belangenafweging in de BIO

De BIO biedt de basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt en legt de verantwoordelijkheid hiervoor bij het lijnmanagement. Het beveiligen van informatie is een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Dit is een continu proces, wat volgens de *plan-do-check-act cyclus* wordt doorlopen. De BIO maakt gebruik van een methode om vast te stellen welke informatie en informatiesystemen dermate belangrijk zijn, dat hier een extra beveiliging voor moet worden ingericht. Door middel van *risicomanagement* wordt voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd. De BIO beschrijft een proces om te komen tot een passende beveiliging van informatie en informatiesystemen.

Allereerst wordt er een *risicoafweging* gemaakt waarbij de mogelijke schade wordt ingeschat wanneer een informatiesysteem tijdelijk niet *beschikbaar* is, informatie niet langer *integer* is of wanneer informatie in verkeerde handen valt. Daarnaast wordt er een inschatting gemaakt van de dreigingen waartegen de overheid beschermd moet worden. Dit samen leidt tot beveiligingseisen om het risico te beperken. Door middel van generieke schades en dreigingen zijn voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Er worden drie BBN's onderscheiden, die aan de hand van een BBN-toets worden gekozen voor ieder bedrijfsproces. Per BBN is beschreven aan welke *controls* uit de ISO27002[59] moet worden voldaan en hoe aan de beveiligingsdoelstelling kan worden voldaan. Waar van toepassing zijn controls uitgewerkt in verplichte, concrete overheidsmaatregelen.

BBN-toets

De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen beschikbaarheid, integriteit en vertrouwelijkheid. De BBN-toets helpt bij het kiezen van het best passende niveau.[60] Bij het uitvoeren van de BBN-toets wordt BBN2 als uitgangspunt genomen voor alle informatiesystemen. De toets bestaat uit drie stappen. In stap 1 wordt getoetst of de beveiligingseisen die vallen onder BBN2 voldoende zijn. Om dit vast te stellen wordt antwoord gegeven op de vragen die te vinden zijn in Figuur 4[61]. Nadat de BBN-toets is uitgevoerd doorloopt het lijnmanagement de 'controls'[62]. Op basis van een risicoafweging wordt bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor een deel van deze controls gelden verplichte maatregelen, ook wel 'overheidsmaatregelen' genoemd in de BIO. Hiervan is sprake wanneer 1) deze maatregelen voortvloeien uit wet- en regelgeving; 2) deze maatregelen zo basaal zijn

[59] ISO 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. Met ISO 27001 certificering laat een organisatie zien dat zij voldoet aan alle eisen rondom informatiebeveiliging. Deze standaard is een *best practice* om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening.
[60] Voor een overzicht van de beschikbaarheids-, integriteits-, en vertrouwelijkheidsniveau per BBN zie BIO Versie 1, p 66-68.
[61] BIO Versie 1, p. 17-18.
[62] De Nederlandse versie van ISO 27002 spreekt van beheersmaatregelen. Er zijn echter ook implementatiemaatregelen. Om het onderscheid daartussen makkelijker te maken, hanteert de BIO de Engelse term 'controls'. Het gebruik van deze term sluit aan bij de informatiebeveiligingspraktijk.

dat zij het fundament vormen van een betrouwbare c.q. professionele informatievoorziening; of 3) wanneer deze maatregelen dienstbaar zijn aan de beveiliging in een procesketen of netwerk. Niet-naleving is in dit laatste geval ineffectief voor de gehele keten.

BBN1	• Wordt gekozen wanneer blijkt dat de maatregelen van BBN2 te zwaar zijn. Dit geldt voor systemen waarbij bovenstaande schades niet aan de orde zijn.
BBN2	• Wordt gekozen voor specifieke informatiesystemen. Hiervoor wordt gekeken naar de mogelijke schade van het openbare van informatie. • Er wordt gekozen voor BBN2 indien er sprake is van: o Politieke schade aan een bestuurder: bestuurder moet verantwoording afleggen aan de (gekozen) controlerende organen, bijvoorbeeld naar aanleiding van verantwoordingsvragen. o Diplomatieke schade te herstellen door ambtelijke opschaling. o Financiële gevolgen: niet meer op te vangen binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven. o Verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers. o Bindende aanwijzing van de Autoriteit Persoonsgegevens in verband met schending van de privacy o Directe imagoschade, bijvoorbeeld door negatieve publiciteit
BBN3	• Wordt gekozen wanneer uit de BBN-toets blijkt dat BBN2 onvoldoende is. • Er wordt gekozen voor BBN3 indien er sprake is van: o De informatie beschermd dient te worden tegen statelijke actoren of vergelijkbare dreigers; o Informatie wordt geleverd door derden en deze voor de beveiliging van betreffende informatie BBN3 eisen; o Aansluiting op een infrastructuur het BBN3 vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen).

Figuur 4: BBN-toets

De redeneerlijn om te komen tot BBN3 gaat uit van risico/dreiging of van een door derden opgelegde verplichting, en niet van een afweging van het belang van de te beschermen informatie. De beveiligingsmaatregelen die organisaties moeten nemen die informatie, gegevens of registraties verwerken die kunnen worden aangemerkt als van Nationaal Belang zouden wel goed kunnen aansluiten op BBN3 (zie ook het volgende hoofdstuk).

Verantwoording

- De Secretaris of Algemeen Directeur van een organisatie is de eindverantwoordelijke voor de inrichting en werking van de beveiligingsorganisatie.[63] Dit betekent dat hij/zij eindverantwoordelijk is voor de implementatie van de beveiligingskaders van de organisatie en daarmee voor de juiste toepassing van de BIO. De ISO 27001 en het VIR bepalen dat het lijnmanagement vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd.[64] De invulling van deze verantwoording is afhankelijk van het vastgestelde BBN-niveau. Hoe hoger het BBN-niveau, hoe hoger de potentiële impact en de noodzaak om gedetailleerd te rapporteren en te verantwoorden. Op basis van het vastgestelde beveiligingsniveau wordt de verantwoordelijkheid voor risicomanagement als volgt belegd.[65]

[63] Zie: Artikel 4 lid 1 Beveiligingsvoorschrift Rijk.
[64] Zie: Artikel 4 sub b VIR.
[65] Zie: BIO Versie 1.

- Voor BBN1 is de proceseigenaar volledig verantwoordelijk voor het nemen van (verstandige) beslissingen. Slechts incidenteel en op verzoek informeert deze de CISO over de stand van zaken met betrekking tot zijn BBN1-informatiesystemen.
- Voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp-/ontwikkelfase) ter consultatie voorlegt aan de CISO).[66]
- Voor BBN3 geldt dat vooraf toestemming verleend moet worden door de secretaris/algemeen directeur voor het verwerken van bijzondere informatie (conform het VIRBI 2013).[67] Voor het verlenen van toestemming is mandatering mogelijk naar bijvoorbeeld de CIO of CISO en bij het Rijk naar de BVA. Organisaties kunnen voor BBN1 en BBN2 hiervan afwijken in het informatiebeveiligingsbeleid.

De BIO kiest voor een diepgang van de *controls*, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime dat proportioneel is aan de vereiste beveiliging in combinatie met relevante dreigingen. Hiervoor onderscheidt de BIO drie basisbeveiligingsniveaus, waarbij niveau BBN2 als uitgangspositie wordt genomen en van waaruit de noodzaak wordt getoetst om eisen aan te scherpen of te versoepelen. Ook voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. De methodiek, die vanuit de BIO wordt toegepast om een mate van informatiebeveiliging vast te stellen op basis van de mogelijke schade bij (tijdelijk) ontbreken van beschikbaarheid en mogelijke dreiging voor de overheid is primair gericht op het afwegen van de proportionaliteit tussen het te beschermen belang en de te nemen beveiligingsmaatregelen. Ook bij deze methode wegen organisaties zelf het belang en schatten zij zelf de risico's in. De kans bestaat ook hier dat individuele organisaties verschillende interpretaties hebben van bepaalde belangen en dat het erg afhankelijk is van bijvoorbeeld de positie van voor informatiebeveiliging verantwoordelijke functionarissen, de mate van volwassenheid van een organisatie op het gebied van informatiebeveiliging en de prioriteit en het gewicht dat door de leiding van een organisatie aan informatiebeveiliging wordt toegekend hoe belangen worden gewogen, hoe risico's worden ingeschat en of adequate maatregelen worden genomen. Dat is een kwetsbare systematiek voor gegevens, documenten en registraties die ook (juist) voor organisaties buiten de eigen organisatie van cruciaal belang zijn, die zelfs van Nationaal Belang zijn.

3.5. Andere aanknopingspunten voor het identificeren en wegen van belangen

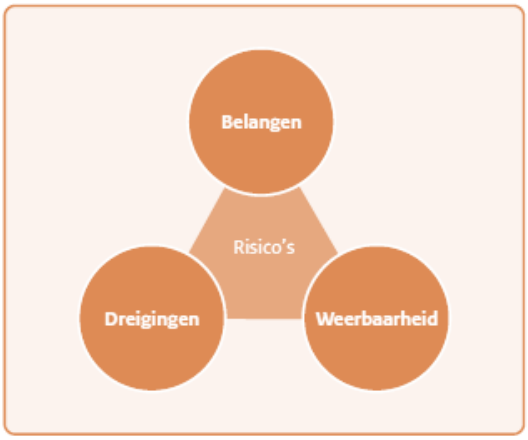
Zicht en grip op de risico's rondom informatie: waarde van informatie als uitgangspunt
Het NCSC stelt in de factsheet *Risico's beheersen: de waarde van informatie als uitgangspunt*[68]dat goed zicht hebben op informatie noodzakelijk is om deze te kunnen beheren. Voor het maken van een overzicht van de relevante informatie binnen een organisatie zijn volgens het NCSC de primaire en andere belangrijke bedrijfsprocessen een goed uitgangspunt. De afdeling informatiemanagement is de aangewezen partij om het verkrijgen van inzicht in het informatielandschap te coördineren. Dat inzichtelijk maken van informatie moet zich niet beperken tot informatie binnen de organisatie: informatie waar de organisatie verantwoordelijk voor is, kan opgeslagen liggen bij externe partijen. Ook kan de organisatie in zekere mate afhankelijk zijn van informatie uit externe bronnen. Het NCSC adviseert om dit soort informatie mee te nemen in het overzicht. Als we deze aanbeveling vertalen naar de overheid dan is er een grote gelijkenis met de aanbeveling van de WRR om een *Cyberafhankelijkheidsbeeld* op te stellen (zie hoofdstuk 1).

Nationale Cybersecuritystrategie en Veiligheidsstrategie voor het Koninkrijk der Nederlanden
Nadat zicht en grip op informatie is verkregen, kan gewerkt worden aan het krijgen van zicht en grip op de beveiliging daarvan. Dat kan volgens het NCSC met een risicoanalyse binnen een risicomanagement dat is ingericht en wordt

[66] Voor DepV informatie geldt, conform het VIRBI, het BBN3-regime voor verantwoording.
[67] Zie: Artikel 3 sub b VIR-BI.
[68] NCSC, Risico's beheersen: de waarde van informatie als uitgangspunt. Over eigenaarschap en verantwoordelijkheden (Factsheet FS-2020-04, versie 1.2, februari 2023).

uitgevoerd zoals aangegeven in de ISO 31000 norm en - specifiek voor informatiebeveiliging - in de ISO 27005-norm. Op basis van de risicoanalyse kunnen voor niet-acceptabele risico's vervolgens maatregelen worden geformuleerd en geïmplementeerd. Tegelijkertijd constateert de *Nederlandse Cybersecuritystrategie 2022-2028 (NLCS)*[69] dat samenhangend en geïntegreerd (digitaal) risicomanagement nog in de kinderschoenen staat: "Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal staat nog in de kinderschoenen. Digitale risico's hebben nog geen structurele plaats in het bredere risicomanagement binnen en tussen de drie eerdergenoemde niveaus. Risicomanagement is nog niet vanzelfsprekend, terwijl een risico-gebaseerde manier van werken instrumenteel is voor het bepalen en op het gewenste niveau brengen van de weerbaarheid. Uiteraard hebben talrijke organisaties hun risicomanagement op orde. Toch schort het binnen organisaties vaak aan inbedding in het primaire proces."

Digitale risico's worden volgens de NLCS bepaald door de samenhang tussen belangen, de dreiging daartegen en de weerbaarheid (zie Figuur 5):



Figuur 5: Risico's als resultante van belangen, dreigingen en weerbaarheid

Door technologische ontwikkelingen en vergaande digitalisering van de maatschappij neemt het belang van digitale processen toe. Digitale processen vormen het 'zenuwstelsel' van de maatschappij en economie, omdat ze onmisbaar zijn voor het ongestoord functioneren daarvan. Digitale veiligheid is volgens de NLCS dan ook onlosmakelijk verbonden met de nationale veiligheidsbelangen. De zes nationale veiligheidsbelangen zijn: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit en internationale rechtsorde. De zes nationale veiligheidsbelangen, zoals beschreven in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden[70] kunnen ieder worden geraakt via de digitale ruimte. Hoe deze belangen zich ten opzichte van elkaar verhouden – of het ene belang, soms, zwaarder kan wegen dan het andere – wordt niet duidelijk. Belangen kunnen ook over tijd wijzigen: tussen 2007 en 2016 was nog sprake van 5 nationale veiligheidsbelangen ('politieke stabiliteit en internationale rechtsorde' werd nog niet als zodanig, apart onderkend).

Ook in de *Veiligheidsstrategie voor het Koninkrijk der Nederlanden* staan de 6 nationale veiligheidsbelangen centraal: "Wanneer we spreken over nationale veiligheid staan de veiligheidsbelangen die we proactief willen beschermen en bevorderen centraal. Deze veiligheidsbelangen kunnen geschaad worden door dreigingen, wat maatschappelijke ontwrichting kan veroorzaken." Hoe belangen te wegen noch hoe tot deze 6 belangen is gekomen wordt in de verschillende documenten waarop cybersecuritystrategie en veiligheidsstrategie zijn gebouwd uiteengezet. De belangen

[69] Nederlandse Cybersecuritystrategie 2022-2028. Ambities en acties voor een digitaal veilige samenleving (oktober 2022).
[70] Zie: De Veiligheidsstrategie voor het Koninkrijk der Nederlanden, 2023, p. 11.

zijn een gegeven, geïdentificeerde dreigingen en de mogelijke impact ervan worden wel enigszins gewogen (in termen van voorstelbaarheid en ernst). Uiteraard zijn Nationale veiligheidsbelangen van een andere orde dan de Nationale digitale belangen waar dit onderzoek op ziet. We relevant is dat risico's ook hier een relatie hebben met het te beschermen belang en dat gestreefd is naar een totaalbeeld van zowel belangen als dreigingen en de weerstand daartegen.

Bescherming vitale infrastructuur
De Minister van Justitie en Veiligheid heeft op 17 mei 2023 in een brief aan de Tweede Kamer[71] de versterkte aanpak bescherming vitale infrastructuur toegelicht. Aanleiding is dat het beschermen van de weerbaarheid van vitale infrastructuur steeds complexer wordt door de toenemende dreiging van statelijke actoren en cybercriminelen en dat de groeiende digitale verwevenheid en complexe ketenafhankelijkheden vragen om nieuwe oplossingen en aanvullende maatregelen. In de brief wordt opgemerkt – in lijn met de redeneerlijn voor Nationaal Belang – dat de te beschermen belangen - vitale infrastructuur - niet statisch van aard zijn, maar continu onderhevig zijn aan maatschappelijke, internationale en technologische ontwikkelingen. Daarnaast wordt niet (langer) uitsluitend gekeken naar de mate van impact van uitval, verstoring of manipulatie van een proces of dienst op de veiligheid van Nederland, maar zal er (ook) aandacht zijn voor de bredere EU- en NAVO-belangen[72], dit omdat de vitale infrastructuur een sterke internationale verwevenheid kent en de verschillende nationale en internationale processen in grote mate van elkaar afhankelijk zijn.

De Nederlandse vitale infrastructuur bestaat uit die processen die zo essentieel zijn voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Ons elektriciteitsnetwerk, toegang tot internet, drinkwater en betalingsverkeer zijn voorbeelden van vitale processen[73]. Er is onderscheid gemaakt tussen een categorie A en een categorie B in vitale processen om recht te doen aan de diversiteit binnen de vitale infrastructuur, om te kunnen prioriteren bij onder andere incidenten en om maatwerk bij weerbaarheidsverhogende maatregelen mogelijk te maken.

De beoordeling of een proces of dienst vitaal is, wordt gemaakt door het verantwoordelijke vakdepartement, in overleg met de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Hierbij wordt geanalyseerd of bij verstoring, uitval of manipulatie van een proces of dienst dermate ernstige gevolgen kunnen optreden dat deze de nationale veiligheid kunnen schaden. Aan de hand van specifieke criteria en drempelwaarden wordt de potentiële impact van uitval of verstoring van het proces bepaald. Het vakdepartement stelt algemene kaders vast voor de vitale sectoren die onder haar systeemverantwoordelijkheid vallen. Daarnaast kunnen vakdepartementen beleid of sectorale regelgeving ontwikkelen om de weerbaarheid van sectoren te verhogen. Toezichthouders zijn belast met het toezicht op de naleving van de wettelijke verplichtingen[74]. Dit is een cyclisch proces omdat vitale processen constant onderhevig zijn aan ontwikkelingen en het verhogen van de weerbaarheid een continu proces is.

Zoals gezegd wordt bij het beoordelen of een proces vitaal is en daarmee onderdeel uitmaakt van de vitale infrastructuur bepaald door het risico dat *uitval of verstoring* ervan heeft op de nationale veiligheid. De nationale veiligheid is in het geding als één of meer van de zes nationale veiligheidsbelangen (zie hiervoor) zodanig worden bedreigd dat er sprake is van (potentiële) maatschappelijke ontwrichting.

Vitale overheidsprocessen en Nationale Belangen zullen een zekere overlap hebben, maar zijn niet hetzelfde. Ten eerste zijn Nationale Belangen geen processen maar informatie-objecten die een rol kunnen spelen in overheidsprocessen, ook vitale processen. Nationale Belangen zijn niet constant aan ontwikkeling onderhevig, maar kunnen wel constant in zich

[71] Zie: Kamerbrief over versterkte aanpak bescherming vitale infrastructuur.
[72] Welke deze belangen zijn wordt niet nader geduid.
[73] Zie voor meer informatie: Vitale Infrastructuur.
[74] Beschrijving van vitaalbeoordeling overgenomen uit: Kamerbrief over versterkte aanpak bescherming vitale infrastructuur.

ontwikkelende en nieuwe overheidsprocessen worden verwerkt. Sommige Nationale Belangen kunnen ook worden aangemerkt als vitaal, maar niet alle Nationale Belangen hoeven vitaal te zijn of in vitale overheidsprocessen verwerkt te worden. Tot slot lijkt ook sprake van een verschil in abstractieniveau: een Nationaal Belang (bijvoorbeeld een basisregistratie) lijkt een concept van een andere orde dan een nationaal veiligheidsbelang, bijvoorbeeld territoriale veiligheid).

High Value Datasets
Op het Nationale Dataportaal van de Nederlandse overheid, data.overheid.nl, is een register dat hulp biedt bij het openen en hergebruik van data van de overheid. Inmiddels zijn meer dan 16.000 datasets opgenomen in het register. Het kabinet heeft de ambitie om zoveel mogelijk overheidsgegevens als open data beschikbaar te stellen. Daarbij geeft het kabinet prioriteit aan '*High Value*'-*Datasets*. Dit zijn datasets met hoge waarde voor de samenleving, zoals de Basisregistratie Adressen Gebouwen en de kadastrale kaart. Bij het beschikbaar stellen van data wordt prioriteit gegeven aan de ontsluiting van deze datasets. In 2016 heeft data.overheid.nl in samenwerking met gemeenten, de Digitale Stedenagenda en VNG/KING een Gemeentelijke High Value Lijst opgesteld. Deze lijst is voor gemeenten een startpunt om te beginnen met het openen van datasets. Tevens zijn de provincies in 2019 gekomen tot een Provinciale High Value lijst. Op data.overheid.nl zijn high value-datasets gemarkeerd. Datasets die voldoen aan de volgende criteria worden als 'high value' aangemerkt op data.overheid.nl:

- De data is bij de data-inventarisatie door een departement als 'high value' aangemerkt en wordt met hoge prioriteit ontsloten;
- De data komt voor in de gemeentelijke of provinciale high value-lijst.

Of een dataset 'high value' is, wordt bepaald door de mate waarbij de data bijdraagt aan:

- Transparantie
- Wettelijke plicht
- Kostenbesparing
- Doelgroep
- Potentie van hergebruik

Deze criteria worden niet verder uitgewerkt. Dat kan maken dat een zekere subjectieve invulling van zowel de 5 aspecten waaraan data kan bijdragen als 'mate van bijdragen aan' niet kan worden uitgesloten. Wel wordt op de website verwezen naar internationale voorbeelden van datasets die aldaar als 'high value' zijn aangemerkt.

3.6. Criteria voor het afwegen van belangen

De eerste deelvraag van dit onderzoek luidt: *Welke eenvoudige en onbetwiste criteria leiden tot een Nationaal Belang?* Zowel in literatuur als in de interviews die we hebben gehouden hebben we geen onbetwiste afwegingsmethodiek noch eenvoudige en onbetwiste criteria kunnen identificeren. In de meeste gesprekken werd – net als in de meeste bestaande systematieken, frameworks en wet- en regelgeving – uitgegaan van risico's en dreigingen, niet van het belang. Bovendien worden die risico's veelal primair bepaald vanuit het perspectief van de eigen organisatie, niet vanuit het belang van ketens en netwerken en al helemaal niet op nationaal niveau. Daarmee wordt minder of geen nadruk gelegd op het belang van gegevens, documenten en registraties voor andere organisaties en processen in ketens en netwerken, laat staan op iets als een Nationaal Belang.

Dit onderzoek beoogt bij te dragen aan het ontwikkelen van een *generiek gemeenschappelijk kader* voor het kunnen bepalen welke gegevens, documenten en registraties kunnen worden aangemerkt als van Nationaal belang. Daarmee heeft dit onderzoek een bredere insteek dan een vitaal beoordeling, omdat het gewenste proces ook belangen

identificeert die naar hun *aard* belangrijk zijn. Bijvoorbeeld, als een rubricering wordt aangebracht op een document, dan is dat document op zichzelf al belangrijk genoeg om te beveiligen, ongeacht het proces, de route of organisaties die dat document volgt.

Door aan te sluiten bij intrinsiek belang in plaats van een afweging van belang, dreiging en weerstand (risicobenadering) én door te benadrukken dat het ziet op relatief onveranderlijke, herkenbare entiteiten waarvan het belang dat van een individuele overheidsorganisatie en -laag en zelfs dat van de gehele overheid overstijgt, komen we tot de volgende criteria:

Criteria voor gegevens, documenten en registraties van Nationaal Belang:

- Het betreft op zichzelf staande informatie-elementen of -objecten van de overheid: gegevens, documenten en registraties[75];
- Deze gegevens, documenten en registraties hebben een grote mate van onveranderlijkheid (wat niet geldt voor processen en systemen);
- Gegevens, documenten en registraties van Nationaal Belang hebben een intrinsiek belang voor meerdere of alle overheidsorganisaties, voor veel of alle burgers en bedrijven, en/of zelfs voor de gehele Staat. Vanwege hun uniciteit, authenticiteit, vertrouwelijkheid, beschikbaarheid of een combinatie van die aspecten vormen ze een cruciaal element in het betrouwbaar en rechtmatig kunnen handelen van de Nederlandse Staat en/of de Nederlands overheid en/of grote delen van de maatschappij. In geval van compromitteren, of de mogelijkheid van compromitteren kan grote schade ontstaan voor de Staat, voor zijn bondgenoten en/of voor grote delen van de maatschappij.

Door het laatste criterium benadrukt de overheid ook het belang van gegevens, documenten en registraties die door de overheid worden verwerkt voor Staat en maatschappij. De *Veiligheidsstrategie voor het Koninkrijk der Nederlanden* (2023, p. 17)[76] hierover: "Voldoende legitimiteit en draagvlak zijn nodig voor het goed functioneren van onze democratische rechtsorde. Veel burgers zijn kritisch op de politiek, bijvoorbeeld omdat zij van mening zijn dat de politiek onvoldoende met oplossingen komt voor de maatschappelijke problemen. Kritiek, debat en protest horen bij het samenleven in een democratie. Problematisch wordt het als mensen definitief afhaken en hiernaar gaan handelen, bijvoorbeeld omdat hun wantrouwen structureel is. […] De wijze waarop (overheids-)instituties communiceren heeft directe invloed op het toenemen of wegnemen van wantrouwen. […] Binnen de protesten die een bijdrage leveren aan de democratische rechtsorde, beweegt zich echter een radicale onderstroom. Een voorbeeld hiervan zijn extremisten die zich vanuit een fundamenteel wantrouwen, woede en onrechtvaardigheidsgevoel tegen de overheid en andere instituties richten. […] Ze verzetten zich tegen de manier waarop de politiek, het rechtssysteem, de media en de wetenschap worden ingevuld. Een deel van hen omarmt complottheorieën of deelt zelfs structureel desinformatie. [...] Complottheorieën doen afbreuk aan het publieke vertrouwen in de democratische rechtsorde. Dergelijke afbreuk is niet direct merkbaar maar manifesteert zich sluipenderwijs. Daarbij komt dat burgers meningen vormen en keuzes maken op basis van de informatie die wordt verspreid binnen het publieke debat. De verspreiding van desinformatie, uit zowel binnen- als buitenland, kan dit publieke debat verstoren en een ontwrichtend effect hebben op de samenleving en de levens van individuele mensen daarin."

De overheid kan bijdragen aan het zorgen voor betrouwbare gegevens en documenten en als bron van feiten en waarheid dienen, maar dan dient het wel te zorgen voor betrouwbare, beschikbare gegevens en documenten. Dit dient niet alleen betrouwbare overheidsprocessen en betrouwbare dienstverlening aan burgers en bedrijven, maar ook als

[75] Waar we in dit rapport spreken van document wordt eigenlijk bedoeld: informatieobject. En informatieobject is een op zichzelf staand geheel van gegevens met een eigen identiteit. Voorbeelden van informatieobjecten/documenten zijn brief, e-mail, video, webpagina, tweet, subsidieaanvraag, vergunning. Registraties zijn databronnen met een wettelijke grondslag. Overheidsorganisaties hebben een wettelijke taak om bepaalde gegevens te verzamelen en te registeren in zogenaamde registraties. Een aantal registraties van de overheid is aangewezen als Nationale Basisregistratie. Zie ook Bijlage 1.
[76] De Veiligheidsstrategie voor het Koninkrijk der Nederlanden, 2023, p. 17.

belangrijk middel tegen desinformatie. Het beveiligen van de belangrijkste gegevens, documenten en registraties is dan cruciaal.

Deze criteria leiden tot de volgende generieke categorieën gegevens, documenten en registraties van Nationaal Belang:

- **Bijzondere (gerubriceerde) informatie**
  Alle bijzondere (gerubriceerde) informatie die valt onder het VIRBI 2013, of onder een internationaal verdrag of overeenkomst van tenminste het niveau Stg.GEHEIM en gegevens die zijn opgeslagen in een verboden plaats.[77]
- **Nationale Basisregistraties**
  Alle nationale (basis)registraties - waaronder in elk geval alle basisregistraties – met een wettelijke basis, die cruciale, authentieke gegevens en/of documenten bevatten over personen, organisaties, gebouwen, geografie en economie.[78] Ook de registraties met koppelgegevens, die gegevens van de ene registratie aan gegevens van een andere registratie koppelen, vallen hieronder als het om een koppeling met een registratie van Nationaal Belang gaat.[79] Hierbij zijn ook de voorzieningen om deze registraties te raadplegen belangrijk. Deze voorzieningen (met een wettelijke basis) die gegevens raadplegen die van Nationaal Belang zijn, moeten voldoen aan een aantal vereisten.
- **Overige (documenten en) registraties[80] van Nationaal Belang**
  Andere (documenten en) registraties kunnen volgens een systematiek identiek aan het afwegen van belangen van het Nationaal Archief (zie ook de paragraaf hierna over vaststellen van Nationale Belangen) worden voorgedragen om ook te worden vastgesteld als Nationaal Belang. Hierbij kan worden gedacht aan registraties/datasets van de overheid waarvan het aantal snel groeit en waarvan enkele de functie van lokale bestanden (al dan niet analoog) hebben overgenomen. Door op één punt digitaal beschikbaar te worden kan de waarde en daarmee het gebruik van dergelijke registraties snel toenemen. Daarmee kan zelfs een zekere afhankelijkheid groeien. Wanneer tegelijkertijd niet kan worden teruggevallen op de initiële lokale bestanden, kan een dergelijke registratie een toenemend belang krijgen dat het lokale/regionale overstijgt. Hierbij zou kunnen worden gedacht aan registraties van de Rechtspraak.
- **Overige gegevens, documenten en registraties (al dan niet tijdelijk) op basis van een politieke belangenafweging**
  Naar aanleiding van een *politieke* belangenafweging kunnen overige gegevens, registraties en documenten van de overheid door de Minister van BZK (ook tijdelijk) tot 'Nationaal Belang' worden verklaard. Dit heeft gelijkenis met de zgn. hotspot-monitor, alleen zullen hier andere criteria moeten worden aangelegd. Gedacht kan worden aan:
  - Een crisissituatie die maakt dat specifieke gegevens, documenten of registraties plots van groter belang worden voor de Staat, de overheid of de maatschappij;
  - Een situatie waarin het vertrouwen in instituties op het spel staat en waarbij de overheid (tijdelijk) maatregelen kan treffen om het vertrouwen in gegevens, documenten of een registratie te garanderen of te herstellen.

[77] Volgens het VIRBI 2013 dient een rubricering te worden "aangebracht op informatie". Ook is voorgeschreven dat een document bij verspreiding ten minste voorzien moet zijn van rubriceringsduur, bladzijdenummering en totaal aantal bladzijden waaruit het document bestaat en in sommige gevallen exemplaarnummer. Door deze maatregelen lijkt het VIRBI 2013 zich nog vooral te richten op klassieke (tekst)documenten. In de definitie van Nationale Belangen is een document feitelijk een informatieobject: een op zichzelf staand geheel van gegevens met een eigen identiteit. Voorbeelden van informatieobjecten/documenten zijn brief, e-mail, video, webpagina, tweet, subsidieaanvraag, vergunning. Het aanbrengen op informatie van een rubricering, rubriceringsduur en bladzijdenummering werkt heel goed voor (tekst)documenten, maar veel minder goed voor een dataset, een tweet, een video of een geluidsfragment. Indien alle (typen) informatie-objecten en registraties ook gerubriceerd moeten kunnen zijn zonder dat dit op 'de informatie' is 'aangebracht' zal onderzocht moeten worden hoe een verplichting om rubriceringsaanduidingen aan (digitale) informatieobjecten te koppelen, bijvoorbeeld als een digitaal watermerk, technisch moet worden vormgegeven – als dit al mogelijk is in alle gevallen, dit zal technisch complex en mogelijk nooit waterdicht zijn en hoogstwaarschijnlijk is het zonder extra handeling/specifieke apparatuur minder duidelijk voor een gebruiker en daardoor voor de (her)kenbaarheid minder bruikbaar. Tot die tijd zullen informatie-objecten waar een rubricering niet eenvoudig en herkenbaar op is aan te brengen op andere wijze herkenbaar moeten worden aangeduid als gerubriceerd.

[78] In het rapport 'Kwaliteitsinformatie Stelsel van Basisregistraties 2021' is zowel informatie over de kwaliteit op stelselniveau, als een overzicht van de gerealiseerde kwaliteit per basisregistratie beschreven.

[79] Denk hierbij aan Digikoppeling, Digimelding en Digilevering. Dit valt onder de dienstverlening van Logius, een agentschap van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

[80] Dit zal voornamelijk andere registraties betreffen, waaronder registraties van onder meer documenten. Bij (individuele) documenten wordt het Nationaal Belang via rubricering aangebracht.

Gegevens, informatie en registraties van Nationaal Belang (de kroonjuwelen van de digitale overheid) zijn per definitie gebonden aan bij het belang en risico passende **eisen**. Of deze 'kroonjuwelen' nu worden gebruikt of niet. Ook als ze 'stilstaan' moeten ze beschermd worden tegen compromitteren, schade of uitval. De Basisregistratie Persoonsgegevens is bijvoorbeeld de **enige** overheidsregistratie van zijn soort met authentieke gegevens. Dit betekent dat - ongeacht of deze wordt gebruikt in een proces - de registratie **100% beschikbaar, integer en vertrouwelijk moet** zijn.

Alle **processen**[81] (en systemen) die gebruikmaken van gegevens, documenten en/of registraties van Nationaal Belang dienen zich te conformeren aan de daarbij behorende normen, maatregelen en bijbehorend toezicht. De mate waarin beveiliging nodig is, hangt af van de aard van de verwerking(shandeling), waarbij raadplegen van gegevens met minder eisen omkleed is dan de mogelijkheid tot muteren of vernietigen van gegevens, maar waarbij raadplegen van Stg.ZEER GEHEIM gerubriceerde documenten weer met meer eisen is omkleed dan raadplegen van Stg.GEHEIM gerubriceerde documenten (meer over maatregelen en toezicht volgt in de volgende hoofdstukken).

Een aantal **voorzieningen van de overheid** kunnen als cruciaal worden aangemerkt voor het beschikbaar stellen en uitwisselen van de belangrijkste gegevens op een wijze die de vertrouwelijkheid, integriteit en beschikbaarheid verzekerd.

3.7. Wie stelt Nationaal Belang vast?

Met Nationaal Belang (kroonjuwelen) wordt verwezen naar de belangrijkste en gevoeligste overheidsinformatie waarvan compromitteren (of kans op compromitteren) leidt tot schade aan de Staat, maar wie bepaalt wat van Nationaal Belang is? Gezien het belang en de consequenties, ligt het voor de hand dat er zicht gehouden wordt op wat wordt aangemerkt als Nationaal Belang. Een voorstel kan zijn om het vaststellen van gegevens, documenten en registraties van Nationaal Belang op centraal, nationaal niveau te beleggen. In bestaande (wettelijke) kaders worden zogenaamde *lijnverantwoordelijken* en *vaststellers* geïdentificeerd.

Situatie nu

Rijksbreed

De Minister van Binnenlandse Zaken en Koninkrijksrelaties stelt een Chief Information Officer Rijk en een Chief Information Security Officer Rijk aan. De **CIO Rijk** is belast met de ontwikkeling en coördinatie van het Rijksbrede informatievoorziening- en digitaliseringsbeleid en draagt zorg voor de ontwikkeling en het beheer van de ICT-voorzieningen en informatiesystemen. In 2019 kondigde de minister van BZK de functie van CISO Rijk aan om zo de coördinatie op informatiebeveiliging binnen de Rijksoverheid structureel te verbeteren. In het 'Besluit CIO-stelsel Rijksoverheid 2021' staat over de functie het volgende: "De **CISO Rijk** is belast met de coördinatie van de maatregelen en het beleid voor de informatiebeveiliging voor zover deze betrekking hebben op de rijksdienst en ressorteert onder de CIO Rijk."[82] *Informatiebeveiliging* heeft hier de volgende definitie: "het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen".[83]

[81] De staatsecretaris zegt hierover het volgende: "Bij een dergelijke zorgplicht past ook aparte aandacht voor de belangrijkste processen. Dat zijn niet alleen de vitale processen, maar juist ook de hierboven genoemde processen die interbestuurlijke eisen stellen én interbestuurlijk toezicht uitoefenen. Voor deze processen wil ik, samen met onze vitale processen en processen waar staatsgeheimen in rondgaan, een hogere mate van zorgvuldigheid bereiken." (Kamerbrief over generiek kader voor vitale digitale processen van de overheid, 29 september 2022, p. 2).
[82] Besluit CIO-stelsel Rijksoverheid 2021
[83] Ibidem.

De CISO Rijk heeft onder andere de volgende taken[84] ten aanzien van digitalisering en informatievoorziening met betrekking tot de rijksdienst:

- het ontwikkelen, coördineren en monitoren van de implementatie en naleving van Rijksbreed informatiebeveiligingsbeleid en -kaders en de wijze waarop de gegevens over de informatiebeveiliging van informatiesystemen door de ministeries worden verstrekt;
- het zorg dragen voor het Rijksbrede informatiebeveiligingsbeleid als onderdeel van het Rijksbrede digitaliserings- en informatievoorzieningsbeleid;
- het in samenwerking met de CISO's en beveiligingsautoriteit Rijk opstellen en actueel houden van het Rijksbrede risicobeeld en calamiteitenplan met betrekking tot informatiebeveiliging.

De Minister van BZK stelt ook een BVA Rijk aan. De **BVA Rijk** is "belast met het bewaken van het integrale karakter en de consistentie van Rijksbrede kaders voor integrale beveiliging, het bevorderen van een interdepartementale aanpak van beveiligingsissues, alsmede het toezicht op de werking van de integrale beveiliging van de Rijksdienst".[85]

De relatie tussen de BVA Rijk, de CIO Rijk en de CISO Rijk zijn als volgt vastgelegd in het Besluit BVA-Stelsel Rijksdienst 2021: "De BVA's, de CIO Rijk en de CISO Rijk verstrekken de BVA Rijk de informatie die naar zijn oordeel redelijkerwijs noodzakelijk is voor de uitoefening van zijn taken op grond van dit besluit."[86]

Onze respondenten geven terug dat het BVA-stelsel vooral belast is met toezicht en dat zij volgens het VIRBI 2013 een adviserende rol hebben richting de Secretaris-Generaal van een departement.

Departementaal

Iedere minister van een departement is verantwoordelijk voor het aanstellen van:

- Een departementale CIO: is belast met de ontwikkeling en coördinatie van het informatievoorzienings- en digitaliseringsbeleid en het zorgdragen voor de ontwikkeling en het beheer van de informatiesystemen van het ministerie conform dit beleid.[87]
- Een departementale CISO: is belast met de ontwikkeling en coördinatie van het departementale informatiebeveiligingsbeleid, bedoeld in artikel 3 van het VIR 2007 en artikel 3 van het VIRBI 2013 en het ondersteunen van het verantwoordelijk lijnmanagement bij de implementatie en naleving hiervan.[88]
- Een departementale BVA: heeft een kader stellende, adviserende en toezichthoudende rol over de integrale beveiliging van het departement. Er kan voor twee of meer ministeries één BVA aangesteld worden.[89]

In de I-strategie Rijk 2021-2025 (2021, p. 26) staat het volgende: "Iedere organisatie van de rijksoverheid is zelfstandig verantwoordelijk voor de beveiliging van informatie en systemen en voor de bescherming van persoonsgegevens. Die verantwoordelijkheid krijgt invulling door sturing vanuit het lijnmanagement, en een security- en privacy-organisatie bij de departementen en haar onderdelen." In het kader van het versterken van besturing staat "Ook gaat besturing over de eisen en verwachtingen over en weer - tussen de CIO's onderling, en vooral ook tussen de CIO en domeinverantwoordelijken - en hoe we het met elkaar organiseren. Daarbij kunnen er vanuit CIO Rijk zeker kaders gesteld worden, maar die zullen er altijd op gericht zijn om de individuele CIO's te ondersteunen in hun taken" (I-strategie Rijk 2021-2025, 2021, p. 112). Er wordt verder beschreven dat het stelsel alleen goed werkt als alle rollen binnen het stelsel helder zijn en als alle stakeholders in het stelsel helder inzicht hebben in de onderlinge verhoudingen.

[84] Voor een overzicht van alle taken zie: Taken CISO Rijk.
[85] Besluit BVA-stelsel Rijksdienst 2021.
[86] Besluit BVA-stelsel Rijksdienst 2021, Artikel 9. Bevoegdheden BVA Rijk.
[87] Besluit CIO-stelsel Rijksdienst 2021, Artikel 3. CIO-functie.
[88] Besluit CIO-stelsel Rijksdienst 2021, Artikel 6. Departementale CISO.
[89] Besluit BVA-stelsel Rijksdienst 2021, Artikel 3. BVA-functie.

Medeoverheden
Bovenstaande functies zijn beschreven voor de Rijksoverheid, maar ook op het niveau van medeoverheden zijn diverse (wettelijke) kaders van toepassing. De BIO, naast de Rijksdienst, ook van toepassing op de provincies, de waterschappen en de gemeenten. In de Handreiking functieprofiel CISO (2020, p. 6) staat het volgende: "Met de invoering van de BIO en het verbindend verklaren van dit normenkader voor de hele overheid, is aanstelling van een CISO niet langer vrijblijvend, maar verplicht geworden. De aanstelling van een CISO is een belangrijke voorwaarde om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen." De BIO beschrijft echter niet hoe de functie ingevuld moet worden.

Medeoverheden zijn bovendien ook gebonden aan ENSIA en de AVG. Dit betekent dat zij ook een ENSIA-coördinator en een Functionaris Gegevensbescherming (FP) moeten aanstellen. Ook andere functionarissen binnen een gemeente zijn verantwoordelijk voor een specifiek deel van de informatiebeveiliging. Vanuit wet- en regelgeving wordt op verschillende onderdelen binnen de gemeentelijke organisatie de aanstelling verplicht van functionarissen, die een privacy- of beveiligingsfunctie uitoefenen. Voorbeelden zijn de privacybeheerder BRP en de beveiligingsfunctionaris Suwinet. Gemeenten mogen ook een Privacy Officer aanstellen. Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de PO verantwoordelijk voor het actualiseren en bewaken van het privacybeleid binnen de gemeente.

Voorstel voor vaststellen van gegevens, documenten en registraties van Nationaal Belang

Bovenstaande functieomschrijvingen laten zien dat er op alle overheidslagen verschillende functionarissen bezig zijn met informatiebeveiliging. Sommige zijn bij wet, norm of besluit verantwoordelijk voor het vaststellen van beleid, uitvoering en of toezicht binnen hun organisatie.

Gegevens, documenten en registraties van Nationaal Belang vervullen een rol in processen, ketens en netwerken binnen de overheid en daarbuiten en hun belang en de eisen die daaraan vervolgens zouden moeten worden gesteld ten aanzien van beveiliging overstijgen het belang van de individuele organisatie die houder is van die gegevens, documenten en registraties van Nationaal Belang. Het is daarom aan te bevelen dat zowel het vaststellen dát gegevens, documenten en registraties van Nationaal Belang zijn áls het toezicht op naleving van bijbehorende eisen centraal, op nationaal niveau (bij het vakdepartement) worden belegd. Hierbij kan aangesloten worden op de praktijk zoals die wordt gebruikt bij het vaststellen van selectielijsten, waarbij de minister van OCW, samen met de minister die het betreft, selectielijsten vaststelt per departement en voor overige overheidsorganen zelf (met uitzondering van Hoge Colleges van Staat – zie ook hierboven onder 3.2):

- **Bijzondere (gerubriceerde) informatie**
  De VIRBI 2013 schrijft het volgende voor: *Vaststellen* van de rubricering wordt gedaan door de minister, staatssecretaris, secretaris-generaal of een door de secretaris-generaal aangewezen rubriceringsambtenaar. Ons voorstel is dit onveranderd te laten *voor het vaststellen van de rubricering* van individuele objecten, maar om het vaststellen *dat* gerubriceerde documenten vanaf een bepaald rubriceringsniveau als Nationaal Belang worden aangemerkt én *wat* vervolgens de eisen zijn aan verwerken, verwerkers, systemen, locaties, etc. vast te laten stellen door de minister van BZK.
- **Nationale Basisregistraties**
  Nationale Basisregistraties met een wettelijke basis zijn volgens deze definitie automatisch van Nationaal Belang. Uit documentenstudie en open bronnen wordt niet duidelijk hoe een basisregistratie deze wettelijke basis krijgt. Maar logischerwijs wordt deze beslissing – in het kader van Nationaal Belang - genomen door de minister of staatsecretaris van het vakdepartement die het betreft met de minister van BZK samen.
- **Overige (documenten en) registraties van Nationaal Belang**

Andere (documenten en) registraties kunnen volgens een systematiek identiek aan het afwegen van belangen van het Nationaal Archief worden voorgedragen als 'van Nationaal Belang'. Een Strategisch Digitaal Gegevens Overleg (SDGO) - de specifieke invulling van dit overleg verschilt per type zorgdrager (departementen, ZBO's en PBO's en decentrale overheden), maar bij de departementen nemen de Chief Information Officer (CIO) en de CISO structureel deel aan het SDGO – maken een belangenafweging en doen eventueel een voorstel voor het tot Nationaal Belang verklaren van (documenten of) een registratie. Hierbij wordt ook een externe deskundige betrokken. De voordracht kan door de met de minister of staatsecretaris van het vakdepartement die het betreft samen met de minister van BZK worden vastgesteld.

- **Overige gegevens, documenten en registraties (al dan niet tijdelijk) op basis van een politieke belangenafweging**
  De minister of staatsecretaris van het vakdepartement die het betreft en de minister van BZK kunnen, naar aanleiding van een politieke belangenafweging (of een systematiek naar analogie van de hotspot-methode bij archiefselectie, zie hierboven), overige gegevens, registraties en documenten van de overheid (*ook tijdelijk*) tot 'Nationaal Belang' verklaren.

3.8. Tussenconclusie

Er bestaat geen universele methode voor het afwegen van belangen. Ook wanneer gekeken wordt naar de methoden en werkwijzen voor het definiëren of afwegen van belangen binnen de overheid komt dit in de meeste gevallen neer op: "van belang is wat de organisatie van belang vindt". Dat gaat in veel gevallen in meer of mindere mate voorbij aan de waarde die buiten de organisatie kan worden gehecht aan specifieke belangen, zeker wanneer het gaat om gegevens, documenten en registraties die in toenemende mate éénmaal worden gemaakt en vervolgens worden (her)gebruikt door verschillende organisaties, overheidsorganisaties op alle lagen én organisaties en personen buiten de overheid, in verschillende processen.

Dit onderzoek beoogt bij te dragen aan het ontwikkelen van een *generiek gemeenschappelijk kader* voor het kunnen bepalen welke gegevens, documenten en registraties kunnen worden aangemerkt als van Nationaal belang. Daarmee wil dit onderzoek belangen identificeren die naar hun *aard* belangrijk zijn, een *intrinsieke waarde* hebben en een zeker mate van onveranderlijkheid hebben. Door aan te sluiten bij intrinsiek belang in plaats van een afweging van belang, dreiging en weerstand (risicobenadering) én door te benadrukken dat het ziet op relatief onveranderlijke, herkenbare entiteiten waarvan het belang dat van een individuele overheidsorganisatie en -laag en zelfs dat van de gehele overheid overstijgt, komen we tot de volgende criteria:

Criteria voor gegevens, documenten en registraties van Nationaal Belang:

- Het betreft op zichzelf staande informatie-elementen of -objecten van de overheid: gegevens, documenten en registraties;
- Deze gegevens, documenten en registraties hebben een grote mate van onveranderlijkheid (wat niet geldt voor processen en systemen);
- Gegevens, documenten en registraties van Nationaal Belang hebben een intrinsiek belang voor meerdere of alle overheidsorganisaties, voor veel of alle burgers en bedrijven en/of zelfs voor de gehele Staat. Vanwege hun uniciteit, authenticiteit, vertrouwelijkheid, beschikbaarheid of een combinatie van die aspecten vormen ze een cruciaal element in het betrouwbaar en rechtmatig kunnen handelen van de Nederlandse Staat en/of de Nederlands overheid en/of grote delen van de maatschappij. In geval van compromitteren, of de mogelijkheid van compromitteren kan grote schade ontstaan voor de Staat, voor zijn bondgenoten en/of voor grote delen van de maatschappij.

Het vaststellen van welke gegevens, documenten en registraties worden aangemerkt als van Nationaal Belang geschiedt door de minister of staatsecretaris van het vakdepartement die het betreft samen met de minister van BZK. De minister

van BZK stelt bovendien vast *dat* gerubriceerde documenten vanaf een bepaald rubriceringsniveau als Nationaal Belang worden aangemerkt én *wat* vervolgens de eisen zijn aan verwerken, verwerkers, systemen, locaties, etc.

4. Maatregelen

Dit hoofdstuk beoogt antwoord te geven op de deelvraag: Welke concrete maatregelen kunnen worden toegekend aan alle gegevens, documenten en registraties van Nationaal Belang? Bij gegevens, documenten en registraties van Nationaal Belang horen minimumkwaliteitseisen aan de informatiebeveiliging en informatie gesteld te worden. Dit betekent dat er eisen gesteld worden aan de beschikbaarheid, integriteit, en vertrouwelijkheid en dat er maatregelen genomen moeten worden om aan deze eisen te (blijven) voldoen.[90]

De bescherming van gegevens, documenten en registraties van Nationaal Belang dient door de overheidslagen heen op eenzelfde wijze en niveau te geschieden en mag niet afhankelijk zijn van de mate waarin individuele organisaties bijvoorbeeld risico's wegen, budgetten toekennen of prioriteiten stellen. Daarom zou niet alleen het vaststellen van Nationale Belangen op nationaal niveau dienen te geschieden, maar zouden ook minimumeisen en maatregelen zoveel mogelijk op nationaal niveau vastgesteld moeten worden. Dit helpt om te zorgen dat alle organisaties hetzelfde omgaan met gegevens, documenten en registraties van Nationaal Belang en daardoor ook gemakkelijk(er) gegevens kunnen delen met organisaties die aan dezelfde eisen (moeten) voldoen. Wel zijn er enkele implicaties bij delen van gegevens (in de ambitie van een federatief gegevensstelsel om gegevens, documenten en registraties juist maar één keer op te slaan en daarna – als bron – voor verschillende toepassingen, in verschillende processen te gebruiken zou delen een steeds minder groot vraagstuk moeten worden). Om gegevens, documenten en registraties van Nationaal Belang te kunnen ontvangen en verwerken, dient de ontvangende organisatie *vooraf* te voldoen aan de eisen die aan verwerking (inclusief ontvangst en opslag) behoren. Ook hier geldt weer dat die eisen anders (veelal lichter) zullen zijn indien het om het raadplegen van één of enkele niet-gerubriceerde gegevens gaat dan wanneer het om muteren van die gegevens gaat of wanneer het gaat om raadplegen van grote sets van gerubriceerde gegevens of documenten. Bij delen gaat het altijd om het delen van een kopie – het origineel blijft (in) de bron. Bij een grote dataset (zoals in het geval van een basisregistratie) betekent dit dat een grote set in kopie wordt geleverd: de initiële registratie blijft intact en blijft ook de enige en authentieke bron, waarvoor alle regels gelden. Voor de set die in kopie wordt geleverd en dus voor de ontvangende partij gelden in elk geval alle reguliere bestaande wet- en regelgeving, zoals de AVG, en verplichtende zelfreguleringen, zoals de BIO, etc., maar mogelijk is de set zodanig van omvang dat ook eisen, zoals aan Nationaal Belang gesteld, blijven gelden. Indien sprake is van gerubriceerde gegevens blijven de VIRBI-eisen uiteraard altijd onverkort van toepassing.

Een aantal voorzieningen van de overheid kunnen als cruciaal worden aangemerkt voor het beschikbaar stellen en uitwisselen van de gegevens, documenten en registraties van Nationaal Belang op een wijze die de vertrouwelijkheid, integriteit en beschikbaarheid verzekerd. Deze voorzieningen zouden verplicht gebruikt moeten worden maar vanwege hun belang is het goed deze overheidsvoorzieningen ook onder hetzelfde toezicht te stellen als de Nationale Belangen. We noemen hieronder enkele van deze cruciale overheidsvoorzieningen, maar ook deze lijst kan worden geactualiseerd als zich nieuwe of andere voorzieningen aandienen. In hoofdstuk 5 gaan we in op toezicht op deze voorzieningen.

Voor alle eisen die worden gesteld aan Nationale Belangen zou moeten gelden: *comply or ask permission.* Dit gaat verder dan *comply or explain*, dat vaak een verantwoording voor afwijking van geadviseerde of voorgeschreven maatregelen achteraf is. Met *comply or ask permission* wordt hier bedoeld: vóór het kunnen verwerken van gegevens, documenten en registraties van Nationaal Belang *moet* voldaan worden aan alle eisen die hieraan worden gesteld. Indien hiervan afgeweken zou moeten worden, dient vóóraf toestemming voor die afwijking en eventueel alternatieve, mitigerende maatregelen te zijn gegeven door de toezichthouder.

[90] CIANA: Confidentiality, Integrity, Availability, Non-Repudiation, and Authentication (Information Assurance, Information Security).

4.1. Gegevens, documenten en registraties van Nationaal Belang worden gelijkgesteld met bijzondere informatie cf. het VIRBI 2013

Gegevens, documenten en registraties van Nationaal Belang worden aangemerkt als *bijzondere informatie*. Er is dan wel een aanvulling nodig op hetgeen het VIRBI 2013 voorschrijft voor bijzondere informatie– eventueel in een nieuwe regeling. Deze aanvulling zou in elk geval maar niet uitsluitend moeten zien op:

- Definities – wat wordt verstaan onder gegevens, documenten/informatieobjecten en registraties, welke categorieën van verwerkingshandelingen worden onderscheiden;
- Reikwijdte: het betreft gegevens, documenten/informatieobjecten en registraties, het ziet op verwerking binnen de gehele overheid: naast de Rijksoverheid ook andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties;
- Beveiligingsbeleid: hoe het vaststellen van wat bijzondere informatie (of Nationaal Belang) verloopt, dat toestemming vooraf nodig is voor verwerking (inclusief *comply or ask permission*) en hoe centraal, nationaal toezicht is ingericht;
- Eisen aan de beveiliging: beveiliging wordt niet langer louter ingericht op basis van risicomanagement, maar kent een aantal minimumnormen. Daarbij wordt niet alleen betrouwbaarheid, maar ook integriteit en beschikbaarheid opgenomen als algemene beveiligingseisen.

Door Nationale Belangen aan te merken als *bijzondere informatie*[91] gelden direct alle bepalingen ten aanzien van het VIRBI 2013 ook voor deze gegevens, documenten en registraties (voor zover deze al niet gelden in het geval van gerubriceerde informatie), als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013) die beide ook onverkort van toepassing zijn[92].

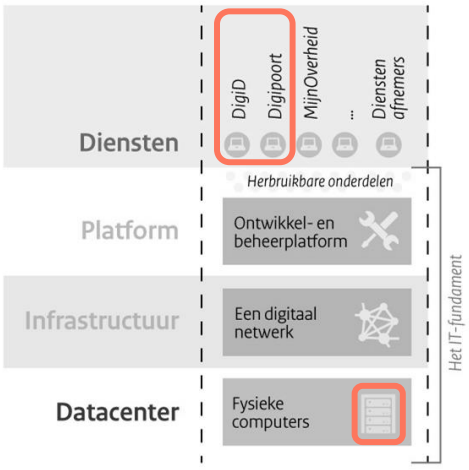
Het VIRBI 2013 is thans alleen van toepassing op de Rijksdienst: de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen. Wellicht kan, om ook gegevens, documenten en registraties van Nationaal Belang onder de werking van het VIRBI 2013 te laten vallen, de reikwijdte worden uitgebreid naar andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties. Dat impliceert bijvoorbeeld dat ook zaken als het (kunnen) toekennen van een rubricering bij andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties moet worden geregeld. Ook dient er ten aanzien van toezicht een aanvulling te komen op het VIRBI 2013: in hoofdstuk 5 wordt voorgesteld om toezicht op (verwerking van) gegevens, documenten en registraties van Nationaal Belang te beleggen bij een onafhankelijke, nationale toezichthouder.

Het is vanuit de verplichting om bijzondere informatie te rubriceren wel zaak om opnieuw te bepalen hoe op gegevens en registraties (en informatie-objecten die een andere verschijningsvorm hebben dan een tekstdocument) een rubricering kan/dient te worden aangebracht.[93] Bovendien zullen mogelijk niet alle documenten en zeker niet alle gegevens in registraties gerubriceerd (kunnen) worden. Daarom zullen ook *niet alle* eisen en maatregelen uit het VIRBI 2013 onverkort van toepassing (kunnen) zijn op *alle* verwerkingshandelingen en gegevensuitwisselingsaspecten: wanneer het bijvoorbeeld gaat om het geautoriseerd kunnen raadplegen of muteren van gegevens in registraties moet dit ook kunnen door personen in omstandigheden die niet aan alle eisen voldoen die het VIRBI 2013 hieraan stelt. Om

[91] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013, artikel 1 onder a. Deze bepaling dient dan wel te worden aangepast/aangevuld.
[92] Zo staat het ook in artikel 2 van het VIRBI 2013.
[93] Zie ook voetnoot 73 op dit punt.

dit werkbaar te maken moet een onderscheid worden gemaakt tussen de verwerking van gerubriceerde documenten (informatie-objecten) en de verwerking van gegevens uit registraties van Nationaal Belang:

- ✓ Voor het verwerken van gerubriceerde documenten (informatie-objecten) gelden onverkort alle eisen uit het VIRBI 2013;
- ✓ Voor het verwerken van gegevens uit registraties van Nationaal Belang geldt dan een zekere gelaagdheid. Deze kan worden toegelicht aan de hand van onderstaande Figuur 6:



Figuur 6: Hoofdlijnen Logius IT-fundament

De data in registraties van Nationaal Belang bevinden zich op de onderste laag: op fysieke computers in datacenters. Voor deze laag gelden alle vereisten van het VIRBI 2013. Ook de vereisten die aan infrastructuur, platform en diensten worden gesteld indien deze worden gebruikt voor (diensten die) gegevens van Nationaal Belang verwerken dienen in beginsel aan de eisen van het VIRBI 2013 te voldoen. Slechts waar in het VIRBI 2013 sprake is van eisen aan digitale verzending van bijzondere informatie (dat dient met ministerieel goedgekeurde cryptografische middelen te geschieden) kan hiervan worden afgeweken. Ook kan worden afgeweken van de eis dat elke persoon die frequent gaat werken met bijzondere informatie voorafgaand aan indiensttreding een aan zijn functievervulling gerelateerd betrouwbaarheidsonderzoek dient te ondergaan: voor personen die betrokken zijn bij de ontwikkeling en instandhouding van ICT-producten en -diensten op alle lagen dient deze eis onverkort te gelden, maar voor gebruikers van data via de verschillende diensten kan dit mogelijk een te vergaande eis zijn.

4.2. Fysieke locatie waar verwerking van gegevens, documenten en registraties van Nationaal Belang plaatsvindt

Onderzoek of het mogelijk en wenselijk is om specifieke locaties, zoals datacenters, aan te kunnen wijzen als verboden plaats.

Het VIRBI 2013 geeft al eisen en maatregelen teneinde te waarborgen dat een toereikende weerstand wordt gerealiseerd tegen (pogingen tot) ongeautoriseerde fysieke toegang van locaties, gebouwen en ruimtes (waaronder kluizen), waar zich bijzondere informatie bevindt. Overwogen kan worden om specifieke plekken, zoals datacenters, aan te wijzen als verboden plaats. Dit kan volgens de Wet bescherming staatsgeheimen[94] uitsluitend ter bescherming van gegevens,

[94] Zie Wet bescherming staatsgeheimen.

waarvan de geheimhouding door het belang van de veiligheid van de staat wordt geboden – bijzondere informatie, zoals gegevens, documenten en registraties van Nationaal Belang zouden daartoe gerekend kunnen worden.

4.3. Gebruik van standaarden en toezicht daarop

Voor alle ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen gelden de (open) standaarden van de 'Pas toe of leg uit-lijst', afwijken kan alleen na expliciete toestemming.

Volgens de Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten[95] dienen bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst die op de website www.forumstandaardisatie.nl is gepubliceerd, te worden gekozen voor een ICT-dienst of een ICT-product dat gebruikt maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard. Van het eerste lid *kan* worden afgeweken indien een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht. Dergelijke afwijkingen van het de open standaarden moeten dan gemotiveerd ('leg uit') worden vastgelegd in de departementale administratie[96]. In de instructie wordt aangegeven dat bij het aanschaffen van ICT-diensten of ICT-producten in veel gevallen sprake zal zijn van een aanbesteding en dat het voor zich spreekt dat in een dergelijk geval de aanbestedingsrechtelijke regels gevolgd moeten worden. Deze instructie geldt nu voor de Rijksdienst en fungeert vervolgens ook als voorbeeld voor andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties voor de wijze waarop zij het gebruik van open standaarden kunnen bevorderen binnen hun eigen organisaties.

Voor alle ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen, kan gelden dat deze dienen te voldoen aan de standaarden van de 'Pas toe of leg uit-lijst', waarmee de verplichting wordt uitgebreid tot andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties. Verder zou kunnen worden bepaald dat voor deze ICT-diensten en ICT-producten niet kan worden volstaan met gemotiveerd vastleggen van afwijkingen van het de open standaarden in de administratie van de organisatie, maar dat een afwijking actief moet worden gemeld bij de toezichthouder. De toezichthouder kan dan bij een ontoelaatbare[97] afwijking adviseren om aanvullende maatregelen te treffen voor, dan wel - via het beëindigen van de levering van (specifieke) diensten[98] - de toegang van gegevens, documenten of registraties van Nationaal Belang te ontzeggen aan de desbetreffende organisatie. Tot slot kan een uitzondering worden gemaakt voor aanbestedingsregels voor ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen – zie hieronder.

4.4. Verplicht gebruik van voorzieningen voor uitwisseling van gegevens van Nationaal Belang

Hieronder volgt een lijst met *overheids*voorzieningen die verplicht zouden moeten worden gebruikt bij de verwerking van gegevens, documenten en registraties van Nationaal Belang. Deze lijst is mogelijk nog niet compleet en mogelijk ook aan verandering onderhevig (o.a. met de migratie naar een nieuwe ICT-infrastructuur door Logius, maar ook met andere ontwikkelingen). Naast deze voorzieningen dient ook te worden voldaan aan bij deze voorzieningen geldende standaarden en afsprakenstelsels, voor zover deze niet al verplicht zijn gesteld in het kader van de 'pas-toe-of-leg-uit-

[95] Besluit van de Staatssecretaris van Economische Zaken van 8 november 2008, nr. WJZ/8157380, tot vaststelling Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten.
[96] Behalve wanneer ICT-diensten of ICT-producten voor militair operationeel gebruik worden aangeschaft.
[97] Hiervoor moeten nadere criteria worden vastgesteld.
[98] Naar analogie van artikel 11.2 van de Algemene Voorwaarden van Logius.

lijst' en waarvoor ook geldt dat hiervan, zoals in de vorige paragraaf benoemd, alleen met expliciete toestemming kan worden afgeweken.

Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Diginetwerk.

Met Diginetwerk kunnen alle organisaties met een publieke taak onderling gegevens uitwisselen om de dienstverlening aan burgers en bedrijven te optimaliseren: makkelijk, veilig en snel. Diginetwerk is een publiek-private samenwerking waarover Logius de regie voert, in opdracht van het ministerie van BZK. Door het besloten karakter is Diginetwerk een veiliger alternatief voor het open internet. Voor het uitwisselen van gegevens van Nationaal Belang door overheden kan Diginetwerk verplicht gesteld worden. Afhankelijk van de gewenste/vereiste beschikbaarheid kan bovendien worden verplicht om één organisatie via meerdere koppelnetwerken aan te sluiten: een redundante aansluiting op Diginetwerk biedt voordelen ten aanzien van risicospreiding.

Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Digipoort.

Bij bedrijfs- of ketenprocessen met grote hoeveelheden berichten en terugkerende stappen in het verwerkingsproces waarvan de procedure vastligt, biedt Digipoort een goede en veilige oplossing. Digipoort is de ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt: Digipoort ontvangt het bericht, controleert het bericht op een aantal eisen en bevestigt – desgewenst – namens de organisatie, de ontvangst van het bericht. Voor gestandaardiseerde (bulk-)bedrijfsprocessen en ketenprocessen waarin gegevens van Nationaal Belang worden verwerkt kan Digipoort verplicht gesteld worden.

Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Digikoppeling.

Digikoppeling is een set van standaarden, die logistieke afspraken bevat voor elektronisch berichtenverkeer tussen (overheids)organisaties. Met Digikoppeling kunnen overheidsorganisaties uniform, veilig, betrouwbaar en efficiënt onderling informatie uitwisselen. Voor gestandaardiseerde (bulk-)bedrijfsprocessen en ketenprocessen waarin gegevens van Nationaal Belang worden verwerkt, kan Digikoppeling verplicht gesteld worden.

Identificatie en authenticaties voor raadplegen van gegevens verloopt verplicht via DigiD.

DigiD is een veilig en betrouwbaar middel waarmee gebruikers zich digitaal kunnen identificeren bij overheidsorganisaties en organisaties met een publieke taak zoals ministeries, lokale overheden, organisaties in de zorg, onderwijs, pensioen en waterschappen. In veel interacties met deze organisaties wordt ook gebruik gemaakt van gegevens uit basisregistraties.

4.5. Aanbesteding van ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen

Voor aanbesteding van ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kunnen uitzonderingen op de Aanbestedingswet en de Aanbestedingswet op defensie- en veiligheidsgebied worden ingezet.

Bij het aanschaffen van ICT-diensten of ICT-producten zal in veel gevallen sprake zijn van een aanbesteding. Ook in gevallen dat het ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen betreft, dienen in beginsel de aanbestedingsrechtelijke regels gevolgd moeten worden.

De Cyber Security Raad pleit in dit kader in haar rapport *Nederlandse strategische autonomie en cybersecurity* voor een meer "gerichte verwervingsstrategie en correcte afweging van uitzonderingsclausules in de Aanbestedingswet 2012[99] en Aanbestedingswet op defensie en veiligheidsgebied."[100]

De Aanbestedingswet 2012 is niet van toepassing op aanbestedingen die geheim zijn verklaard of waarvan de uitvoering overeenkomstig de geldende wettelijke en bestuursrechtelijke bepalingen met bijzondere veiligheidsmaatregelen gepaard moet gaan dan wel indien de bescherming van de wezenlijke belangen van Nederland zulks vereist en deze niet met minder ingrijpende maatregelen kan worden gewaarborgd. Deze uitzondering zou misschien al voldoende kunnen zijn om ICT-diensten en ICT-producten ten behoeve van opslag, verwerking en uitwisseling van gegevens van Nationaal Belang niet via reguliere procedure te hoeven aanbesteden.

Voor deze ICT-diensten en ICT-producten zou bovendien kunnen worden bepaald dat van de reguliere aanbestedingsprocedures afgeweken kan worden door een beroep te doen op de Aanbestedingswet op defensie- en veiligheidsgebied. Als wordt vastgesteld dat gegevens, documenten of een registratie van Nationaal Belang is, hebben deze een bepaald niveau van veiligheidsclassificatie en/of is er een beveiligingsniveau aan toegekend en dienen deze – soms ook in het belang van de nationale veiligheid – uit hoofde van wettelijke voorschriften, van bindende aanwijzingen gegeven vanwege het Rijk of van bestuursrechtelijke besluiten beschermd te worden tegen ontvreemding, vernietiging, verwijdering, onthulling, verlies of toegang tot die gegevens, documenten of registratie door een onbevoegde, of tegen enige andere vorm van compromittering. Daarmee kunnen gegevens, documenten en registraties van Nationaal Belang, voor zover ze dat niet al zijn, gelijkgesteld worden met of gezien worden als gerubriceerde gegevens, bijvoorbeeld door deze aan te merken als *bijzondere informatie:* informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries, zoals gedefinieerd in het VIRBI 2013 (zie hiervoor). Vervolgens kwalificeren materialen, diensten en werken die bestemd zijn voor veiligheidsdoeleinden dat op die gerubriceerde gegevens betrekking heeft, dat gerubriceerde gegevens noodzakelijk maakt, of dat zelf gerubriceerde gegevens bevat als *gevoelige* materialen, diensten en werken. De Aanbestedingswet op defensie- en veiligheidsgebied is van toepassing op het plaatsen van opdrachten voor gevoelige materialen, diensten en werken.[101] In het rapport van de Cyber Security Raad wordt er overigens wel op gewezen dat bij een afweging rekening gehouden moet worden met de interpretatie van het Europese Hof van Justitie in relevante gevallen zoals C-187/16[102] en C-615/10[103].

Het rapport *Nederlandse strategische autonomie en cybersecurity* noemt het aankoopbeleid van de overheid één van de instrumenten om strategische autonomie te versterken. Naast aanbestedingen kan ook gedacht worden aan de mogelijkheid van de overheid om aankopen van cruciale onderdelen door private partijen in kritische infrastructuur te beïnvloeden. Dit kan bijvoorbeeld door:

- ✓ De toepassing van de Algemene Beveiligingseisen Defensieopdrachten 2019104 in bredere zin. Een uitgebreidere toepassing kan een bredere impact hebben op de cyberveiligheid in Nederland en op de strategische autonomie;
- ✓ Aankoop door de overheid van sleutelcomponenten en het verplicht gebruik ervan door operatoren van kritische infrastructuur, zoals in het Nationale Detectie Netwerk;
- ✓ Het opleggen van technische randvoorwaarden aan private operatoren als conditie voor een exploitatievergunning.

[99] Zie: Aanbestedingswet 2012.
[100] Paul Timmers, Freddy Dezeure, *Nederlandse strategische autonomie en cybersecurity* (Cyber Security Raad, januari 2021).
[101] Zie: Artikel 2.1. Aanbestedingswet op defensie- en veiligheidsgebied.
[102] Zie C-187/16.
[103] Zie C-615/10.
[104] Zie: ABDO 2019.

Verder bevat de Algemene Beveiligingseisen Defensie Opdrachten (ABDO) bovendien een plicht om voorgenomen veranderingen in zeggenschap en bedrijfsstructuur te melden. Sinds 2014 is er ook een kabinetsinzet om per vitale sector te kijken of er aanvullende maatregelen nodig zijn om de nationale veiligheid voldoende te borgen bij een overname of investering. Voor elk vitaal proces, wordt een ex-ante analyse uitgevoerd om te kijken of er beschermende maatregelen tegen ongewenste overnames en investeringen moeten worden genomen. Ook dit zou kunnen worden doorgetrokken naar private partijen die betrokken zijn bij ontwikkeling of instandhouding van producten of diensten ten behoeve van de verwerking van gegevens, documenten of registraties van Nationaal Belang.[105]

Onderzoek hoe bij ontwikkelen of aankopen van ICT-diensten en ICT-producten ten behoeve van opslag, verwerking en uitwisseling van gegevens van Nationaal Belang kan worden meegewogen hoe de afhankelijkheid van niet-Europese producten en diensten kan worden beperkt en verplicht mogelijkheden daartoe in aanbestedingen.

Naast veiligheid moet ook het versterken van digitale autonomie expliciet meegewogen worden bij het ontwikkelen of aankopen van om ICT-diensten en ICT-producten ten behoeve van opslag, verwerking en uitwisseling van gegevens van Nationaal Belang. De staatssecretaris voor Koninkrijksrelaties en Digitalisering schrijft in haar *Kamerbrief hoofdlijnen beleid voor digitalisering*[106] dat Nederland en de EU in staat moeten zijn om ook op digitaal terrein hun eigen publieke belangen te behartigen en ongewenste afhankelijkheden voorkomen: "Daarom willen wij waar mogelijk onze open strategische autonomie versterken. Willen we een einde maken aan onze afhankelijkheid van niet-Europese producten en diensten en aansturen op strategische autonomie op Europees niveau. Daarom zetten we naast (Europese) regulering ook in op het ontwikkelen van eigen competenties op het terrein van digitale technologieën, zoals AI en quantum." Juist voor de bescherming van de integriteit, vertrouwelijkheid en de beschikbaarheid van gegevens, documenten of registraties van Nationaal Belang is het cruciaal dat de afhankelijkheid van niet-Europese producten en diensten zo snel mogelijk zo beperkt mogelijk wordt.

4.6. Geëvalueerde producten, Secure Software Development en de Nationale Cryptostrategie

Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht gebruik moeten maken van / bestaan uit door het NBV geëvalueerde producten.

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) ondersteunt de Nederlandse overheid bij het beschermen van gevoelige informatie. Het NBV biedt zijn klanten een reeks van goedgekeurde producten voor de beveiliging van hun digitale informatie. Die goedkeuring wordt pas afgegeven na een evaluatie van het product, waarin onderzocht wordt of het product voldoende bescherming biedt voor de bijzondere informatie: een volledige lijst met goedgekeurde producten is te vinden op de website van het NBV.[107] Het is te overwegen om te onderzoeken of (en welke) ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht door het NBV geëvalueerde producten moeten zijn of uit door het NBV geëvalueerde producten moeten bestaan – voor zover dit niet al gebeurt.

Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht moeten worden ontwikkeld via een proces van Secure Software Development.

Secure Software Development richt zich op het proces van softwareontwikkeling binnen een organisatie. Hierdoor valt SSD buiten de scope van de criteria voor toetsing ter opname op de *'Pas toe of leg uit-lijst'*.[108] De meerwaarde van SSD voor de bouw van veilige software en met name voor software die de bescherming van persoonsgegevens waarborgt,

[105] Zie: Nederlandse strategische autonomie en cybersecurity, 2021, p. 38.
[106] Zie: Kamerbrief 'Hoofdlijnen beleid voor digitalisering' (8 maart 2022).
[107] Zie: Geëvalueerde producten.
[108] Zie: Secure Software Development.

wordt echter terdege onderkend. Het is te overwegen om te onderzoeken of en voor welke ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen, Secure Software Development wellicht een verplichting moet worden.

Onderzoek hoe voor ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kan worden aangesloten op de ontwikkelingen in de Nationale Cryptostrategie.

Vanuit de Nationale Cryptostrategie (NCS) wordt gewerkt aan het versneld ontwikkelen van informatiebeveiligingsproducten voor hoog-gerubriceerde ('bijzondere') informatie en het stimuleren van kennisontwikkeling. Het doel van deze NCS is om de Rijksoverheid te verzekeren van goede en duurzame informatiebeveiligingsmiddelen voor de middellange (drie jaar) en lange termijn (vijf jaar en verder). Bij het vaststellen van prioriteiten trekt de Rijksoverheid op als één partij. Partijen die behoefte hebben aan beveiligingsproducten bundelen de vragen en bepalen samen de urgente behoeftes. Zo wordt gezamenlijk toegewerkt naar een sluitend portfolio voor de hele Rijksoverheid – en daarbuiten. Ook ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen, zouden binnen de scope van dit portfolio kunnen passen (voor zover dit niet al het geval is).

4.7. Overige maatregelen

Voor gegevens, documenten en registraties van Nationaal Belang is het goed om ook na te denken over *worst case scenario's*: kunnen systemen losgekoppeld worden van de infrastructuur (het internet)? Welke alternatieven/back-up bestanden zijn er en waar, en onder welk condities kunnen die worden gebruikt? Zijn er ook nog fysieke alternatieven/back ups, voor zover dat mogelijk en zinvol is? Deze en andere vragen dienen in elk geval te worden gesteld aan gegevens, documenten en registraties van Nationaal Belang en de antwoorden leiden wellicht tot aanvullende maatregelen.

4.8. Strafbaarstelling

Indien ervoor gekozen wordt om gegevens, documenten en registraties van Nationaal Belang onder de werking van het (weliswaar op onderdelen aan te passen) VIRBI 2013 te brengen (en eventueel sommige delen onder te brengen op als verboden plaats aangewezen locaties) dan kunnen schendingen van de integriteit of vertrouwelijkheid van deze gegevens, documenten en registraties voor dat deel onder de werking van artikel 98 tot en met artikel 98c van het Wetboek van Strafrecht komen.

4.9. Tussenconclusie

Ten aanzien van de maatregelen wordt aangesloten bij het VIRBI 2013, waardoor eisen gelden en maatregelen kunnen worden getroffen als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013), die ook onverkort van toepassing zijn. Het VIRBI moet wel op enkele punten worden uitgebreid en aangepast om de reikwijdte uit te breiden naar – naast de Rijksoverheid – andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties – het zal dan mogelijk een andere vorm (wet) krijgen. Ook moet het VIRBI 2017 uitgebreid worden met centraal toezicht.

Verder worden maatregelen voorgesteld die zien op standaarden, verplicht gebruik van overheidsvoorzieningen en aanbestedingen van ICT-diensten en ICT-producten:

Concrete maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang

- Gegevens, documenten en registraties van Nationaal Belang worden aangemerkt als bijzondere informatie: informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries, zoals gedefinieerd in het VIRBI 2013. Het VIRBI dient op enkele punten te worden aangepast en uitgebreid.
- Alle ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen gelden de (open) standaarden van de 'Pas toe of leg uit-lijst', afwijken kan alleen na expliciete toestemming.
- Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Diginetwerk, Digipoort en Digikoppeling
- Identificatie en authenticaties voor raadplegen van gegevens verloopt verplicht via DigiD.
- Voor aanbesteding van ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kunnen uitzonderingen op de Aanbestedingswet en de Aanbestedingswet op defensie- en veiligheidsgebied worden ingezet.

Daarnaast is nog een aantal concrete maatregelen voorstelbaar waarvan de mogelijkheid, wenselijkheid en haalbaarheid nader onderzoek vereist:

Aanbevelingen voor nader onderzoek naar concrete maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang

- Onderzoek of het mogelijk en wenselijk is om specifieke locaties, zoals datacenters, aan te kunnen wijzen als verboden plaats.
- Onderzoek hoe bij ontwikkelen of aankopen van om ICT-diensten en ICT-producten ten behoeve van opslag, verwerking en uitwisseling van gegevens van Nationaal Belang kan worden meegewogen hoe de afhankelijkheid van niet-Europese producten en diensten kan worden beperkt en verplicht mogelijkheden daartoe in aanbestedingen.
- Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht gebruik moeten maken van / bestaan uit door het NBV geëvalueerde producten.
- Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht moeten worden ontwikkeld via een proces van Secure Software Development.
- Onderzoek hoe voor ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kan worden aangesloten op de ontwikkelingen in de Nationale Cryptostrategie.

Er dient nog wel een impactanalyse gemaakt te worden om te onderzoeken of de voorgestelde maatregelen in verhouding staan tot de gewenste niveaus van beveiliging en kwaliteitseisen enerzijds, en de werkbaarheid anderzijds.

5. Toezicht

Er bestaat al langere tijd de wens om het bestaande toezichtstelsel op de digitale overheid te vereenvoudigen.[109] Dit onderzoek wordt uitgevoerd in het kader de voorbereiding van wetgeving, waarin een gemeenschappelijke wettelijke grondslag voor de omgang met en het toezicht op informatieveiligheid wordt geregeld. Directe aanleiding voor het onderzoek vormt de toezegging aan de Tweede Kamer in de *Kamerbrief over de voortgang op informatieveiligheid* van 18 maart 2021[110], om in 2023 een algemeen kader voor vitale systemen op te stellen en zo nodig wettelijk te verankeren. In eerder onderzoek is naar voren gekomen dat voor een aantal van de informatieprocessen van de overheid verticaal interbestuurlijk toezicht op de naleving van deze regels opgezet is.[111] Vooral bij de medeoverheden komen deze regels in de uitvoering weer samen, waardoor zij zich geconfronteerd zien met een grote hoeveelheid gelijksoortige toezicht- en verantwoordingsprocessen.

Het streven is om informatieveiligheid bij de overheid een wettelijke basis te geven. De huidige staatssecretaris wil dit doen via een zorgplicht waaraan nadere regels kunnen worden gesteld zoals de BIO. Zij schrijft "Door het wettelijk verplichten van de BIO is de vrijblijvendheid voorbij". [112] Vanuit de Rijksoverheid worden momenteel vanuit verschillende (wettelijke) kaders informatieveiligheidseisen gesteld aan medeoverheden, bijvoorbeeld voor het gebruikmaken van de BRP en de aansluiting op DigiD. De wens om het bestaande toezicht te vereenvoudigen biedt naast het versimpelen van het toezicht, ook de mogelijkheid om een hogere mate van zorgvuldigheid te bereiken. In de Kamerbrief 'Generiek kader voor vitale digitale processen van de overheid' schrijft de staatssecretaris: "Bij een dergelijke zorgplicht past ook aparte aandacht voor de belangrijkste processen. Dat zijn niet alleen de vitale processen, maar juist ook de hierboven genoemde processen die interbestuurlijke eisen stellen én interbestuurlijk toezicht uitoefenen. Voor deze processen wil ik, samen met onze vitale processen en processen waar staatsgeheimen in rondgaan, een hogere mate van zorgvuldigheid bereiken. Het toezicht moet proportioneel zijn, dus veel aandacht voor de zorgvuldigheid bij het beveiligen van vitale processen en andere 'kroonjuwelen'."

Hoewel er in bestaande wet- en regelgevingen, normen en afsprakenkaders wordt geschreven over toezichtregimes, geven respondenten aan dat deze als onduidelijk worden ervaren, niet centraal geregeld zijn en bovendien niet overal op dezelfde manier worden gehanteerd. De respondenten geven als voorbeeld de uiteenlopende visies over het wettelijk verankeren van de BIO, waarbij tegenstanders aangeven dat het al zou helpen als organisaties de BIO goed implementeren (maar waar een versnipperd toezichtsregime geldt).

Voorgaande hoofdstukken beschrijven de criteria voor Nationale Belangen en welke maatregelen vervolgens getroffen moeten worden. Dit betekent ook iets voor het toezicht. Het hoofdstuk beschrijft eerst hoe het toezicht nu is geregeld en doet daarna een voorstel hoe het toezichtstelsel vereenvoudigd kan worden met oog voor een hoge mate van zorgvuldigheid en proportionaliteit.

[109] Zie onder andere eerdere onderzoeken van Verdonck, Kloosters & Associates (Onderzoek Toezicht en Verantwoording Informatieveiligheid Overheid Horizontaal en verticaal toezicht in balans, 2019; Onderzoek toezicht op informatieveiligheid, 2022).
[110] Kamerbrief voortgang informatieveiligheid overheid, 18 maart 2021.
[111] Onderzoek Wetgevingskader Informatieveiligheid
[112] Generiek kader voor vitale digitale processen van de overheid, 2022, p. 2.

5.1. Toezicht nu

Elke organisatie is zelf verantwoordelijk voor informatieveiligheid en naleving van regels en normen. In eerder onderzoek wordt aangegeven dat "de volwassenheid van een organisatie bepalend is voor het vertrouwen dat daarin gesteld kan worden" (VKA, 2022, p. 11). Op dit moment is voor een aantal vitale ketens reeds gecentraliseerd toezicht ingericht. Voor private partijen wordt het toezicht op grond van de Wbni door onder andere Rijksinspectie voor Digitale Infrastructuur gedaan. Ook bestaat er centraal toezicht op grond van de Wet BRP en houdt de Autoriteit Persoonsgegevens toezicht op de AVG. Deze toezichthouders kijken momenteel ook al naar de genomen beveiligingsmaatregelen.

Zoals eerder beschreven, staat in de BIO dat er voor iedere BBN een verantwoordings- en verantwoordingsregime van toepassing is. Het beschrijft geen toezichtregime. De BIO beschrijft wel dat interne dienstenleveranciers, als onderdeel van de overheid, gehouden zijn aan de reguliere verantwoordings- en toezichtprocedures van de betreffende overheidslagen. Bij het Rijk geldt onder meer het toezicht vanuit de Auditdienst Rijk, Algemene Rekenkamer en de Beveiligingsambtenaar.

De Inspectie Overheidsinformatie en Erfgoed houdt toezicht op de naleving van de Archiefwet en de Erfgoedwet. Zij maakt bij de uitoefening van haar toezichttaak gebruik van een algemeen toezichtkader en van toetsingskaders per toezichtveld. In het Werkprogramma 2023-2024 staat dat de digitale informatievoorziening van de Rijksoverheid razendsnel groeit waardoor het belang van toezicht hierop toeneemt. Hierdoor wordt het toezicht geïntensiveerd. Met extra structurele middelen wordt de Inspectie versterkt.[113] De werkwijze van de Inspectie is als volgt beschreven: "De Inspectie werkt selectief en risico gestuurd. Op basis van informatie uit de Monitor Overheidsinformatie en Erfgoed, vragen en meldingen, de resultaten van uitgevoerde inspecties, de inzichten van beleids- en uitvoerende diensten en het expertoordeel van de inspecteurs wordt een inschatting gemaakt van de belangrijkste risico's per toezichtveld, gebaseerd op wet- en regelgeving. Ontwikkelingen in de maatschappij, politiek, in de toezichtvelden en op het internationale speelveld zijn bepalend voor het selecteren van thema's voor het toezicht. De Inspectie kent een tweejaarlijkse programmering, die wordt vastgelegd in het werkprogramma."[114]

Volgens het BVA-stelsel heeft de BVA een kader stellende, adviserende en *toezichthoudende* rol over de integrale beveiliging van het departement. Tot de taken van de BVA behoort onder andere "het houden van toezicht op de beveiliging van nationale belangen in relatie tot internationale verdragen en richtlijnen; het toezicht houden op de implementatie en werking van de departementale en Rijksbrede kaders van integrale beveiliging en het opstellen van een generiek dreigingsprofiel en een toezichtkader; en het inzichtelijk hebben van kwetsbare functies en toezicht houden op de weerbaarheid tegen ondermijning."[115] De BVA is tevens de ambtenaar die verantwoordelijk is voor het (voorafgaand) toezicht op het waarborgen van een juist beveiligingsniveau gegeven de Te Beschermen Belangen. De BVA is tevens toezichthouder op staatsgeheimen. Het VIRBI 2013 schrijft voor dat de BVA verantwoordelijk is voor het toezicht op de rubricering. Aangezien deze functie niet bestaat bij de medeoverheden is het onduidelijk wie daar de verantwoordelijkheid voor het toezicht heeft.

Bestaande toezichtregimes gaan uit van een bepaalde mate van volwassenheid bij een organisatie en lijken geen rekening te houden met de verschillende lagen (en functies) bij de overheid.

[113] Werkprogramma 2023-2024 Toezicht op informatiehuishouding en digitalisering, omgang met het erfgoed, 2023, p. 6.
[114] Ibidem, p. 7.
[115] Besluit BVA-stelsel Rijksdienst 2021, p. 3

5.2. Toezicht op de 'Kroonjuwelen'

Proportionaliteit

De komst van de NIS2-richtlijn brengt een belangrijke wijziging ten opzichte van de huidige NIS-richtlijn, namelijk dat overheidsdiensten binnen de reikwijdte van de richtlijn worden gebracht en daarmee aan wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen moeten voldoen. Dit geldt in ieder geval voor de rijksoverheid. De conceptrichtlijn stelt verder dat regionale overheden na risicobeoordeling kunnen worden aangewezen. Lidstaten hebben zelf de mogelijkheid om lokale overheden aan te wijzen. Voornemens zijn om lokale overheden, dus gemeenten, waterschappen en provincies, onder de richtlijn te laten vallen. Het Ministerie van BZK is verantwoordelijk voor het organiseren van toezicht op de sector overheid.

De herziene NIS2-richtlijn twee nieuwe categorieën: essentiële aanbieders en belangrijke aanbieders. Bij de essentiële aanbieders, voornamelijk partijen uit Nederlandse vitale sectoren, is het toezicht straks *ex ante* (proactief)). Bij de belangrijke aanbieders vindt het toezicht *ex post* (achteraf) plaats, dus als er aanwijzingen zijn dat er sprake is van een incident. In alle gevallen moet het toezicht 'proportioneel' zijn. NIS2 gaat toezien op digitale en vitale processen.

Deze proportionaliteit betekent dat het wenselijk is om het toezicht op gegevens, documenten en registraties te laten afhangen van het belang. Dit betekent mogelijk dat indien sprake is van belangen op het niveau van Stg. Departementaal Vertrouwelijk het proportioneel is om *ex post* toezicht te regelen. Terwijl naarmate het belang toeneemt, het proportioneel is om *ex ante* toezicht in te regelen. Hierin zijn verschillende lagen denkbaar, zo kan afgesproken worden dat vanaf het niveau Stg.GEHEIM of TBB1 ex ante toezicht proportioneel is. Voor toezicht op gegevens, documenten en registraties van Nationaal Belang zou centraal toezicht kunnen worden ingericht dat vergelijkbaar is met het toezicht op de beveiliging van gerubriceerde informatie van EU en NAVO. Daarbij wordt ingezet op een initiële accreditatie van de betreffende beveiliging bij de overheidspartijen *vóóraf*, aangevuld door periodieke inspecties.

Organiseren van toezicht

Omdat Nationale Belangen raken aan hoogste belangen van de staat, is een vorm van centraal toezicht aan te raden. Deze belangen raken immers altijd de ministeriële verantwoordelijkheid. Zeker bij vitale stelsels die door een groot aantal partijen gebruikt worden is een centraal toezichtkader noodzakelijk.

Om te voorkomen dat de medeoverheden door verschillende toezichthouders worden bevraagd, lijkt het wenselijk om één instantie aan te wijzen, die zowel toezicht houdt bij de Rijksoverheid als bij de medeoverheden. Daarbij komt dat veel van de nationale belangen ook interbestuurlijke effecten hebben omdat ze van Rijk tot medeoverheden of vice versa lopen. Dit maakt het vrijwel onmogelijk om daar een knip te maken in het toezicht.

Binnen de Rijksdienst is door middel van het VIRBI 2013 veel geregeld met betrekking tot bijzondere (gerubriceerde) informatie, maar het VIRBI 2013 biedt geen kader voor andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties. De BVA van een departement is aangewezen als toezichthouder, maar deze functie bestaat niet bij de andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties. Om er zeker van te zijn dat Nationale Belangen ook daar op een uniforme en juiste wijze worden behandeld, moet de verantwoordelijkheid voor deze vorm van informatiebeveiliging binnen andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties belegd worden. Te denken valt aan de CISO.

Het aanstellen van één toezichthouder óók voor medeoverheden maakt het overzichtelijk voor de CISO aan wie hij/zij wanneer wat moet laten zien. Het is denkbaar dat de medeoverheden moeten aantonen dat hun systemen, processen

en medewerkers voldoen aan de eerder beschreven maatregelen voordat zij gegevens, informatie en registraties van Nationaal Belang mogen verwerken.

Het toezicht zou zich overigens ook uit moeten strekken over die overheidsvoorzieningen die verplicht moeten worden gebruikt (ook voor het deel waarbij deze voorzieningen worden aangewend voor toegang of uitwisseling van andere gegevens dan gegevens van Nationaal Belang). In hoofdstuk 4 is een voorlopige opsomming opgenomen van voorziening waarvoor geldt dat gebruik bij verwerken van gegevens, documenten en registraties waar relevant verplicht zou moeten worden gesteld:

- Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Diginetwerk, Digipoort en Digikoppeling;
- Identificatie en authenticaties voor raadplegen van gegevens verloopt verplicht via DigiD.

Omdat dit overheidsvoorzieningen betreft die vrijwel onlosmakelijk verbonden zijn met gegevens, documenten en registraties van Nationaal Belang (maar ook anderszins een cruciale functie vervullen in toegang tot en uitwisseling van gegevens tussen overheden en tussen overheid en derden), ligt het voor de hand het centrale toezicht ook toezicht te laten houden op deze voorzieningen: toezicht op een juiste verwerking van gegevens van Nationaal Belang en op een juiste toepassing daarbij van deze voorzieningen is dan bij één en dezelfde toezichthouder belegd. Of en in welke mate deze nationale toezichthouder ook toezicht zou moeten houden op andere voorzieningen die niet door de overheid maar door derden worden aangeboden, afsprakenstelsels en ander diensten rondom Nationale Belangen zou nader kunnen worden onderzocht.

Randvoorwaarden

Een belangrijke randvoorwaarde voor goed toezicht is dat de centrale toezichthouder toegang heeft tot datgene waarop hij/zij moet toezien. Dit houdt in dat voor de toezichthouder dezelfde beveiligingsmaatregelen en screeningseisen gelden als voor de personele laag die 'kroonjuwelen' mag inzien. Indien het nodig is dat een toezichthouder toegang krijgt tot een verboden plaats, dan dient de toezichthouder hier ook de juiste maatregelen te houden.

De organisaties die gegevens, documenten en registraties van Nationaal Belang beheren of gegevens daaruit verwerken, moeten een bepaalde mate van volwassenheid op het gebied van informatiebeveiliging bereiken. De mate van volwassenheid is immers bepalend voor het vertrouwen dat in de organisatie gesteld kan worden. Een hoge mate van volwassenheid betekent onder andere dat zij in staat zijn om de benodigde capaciteit te organiseren in de vorm van deskundigheid en tijd om de belangenafwegingen correct en navolgbaar te maken en alle maatregel te treffen die zijn vereist en die nodig zijn. Dit betekent ook dat zij de verantwoordelijkheden voor het hoogste niveau van informatiebeveiliging hebben belegd bij de CISO of een andere geschikte eindverantwoordelijke. Het is hierbij wenselijk dat de eindverantwoordelijke voor Nationale Belangen, direct toegang heeft tot de bestuurlijke verantwoordelijke van de organisatie om goed inhoudelijk te kunnen adviseren. Bijvoorbeeld: indien bij de Rijksoverheid ervoor wordt gekozen om de BVA verantwoordelijk is voor Nationaal Belang, dan dient hij of zij direct toegang te hebben tot de SG.

5.3. Tussenconclusie Toezicht

Het Ministerie van BZK is vanuit de NIS2-richtlijn verantwoordelijk voor het organiseren van toezicht op de overheid waarbij de nadrukkelijke wens is om het toezichtstelsel te harmoniseren en te vereenvoudigen zodat een hogere mate van zorgvuldigheid bereikt kan worden. Toezicht is momenteel vanuit (wettelijke) kaders belegd bij verschillende instanties. De komst van NIS2 verplicht om ex ante en ex post toezicht te houden. Voor de verwerking van gegevens, documenten en registraties van Nationaal Belang is het wenselijk om ex ante toezicht te regelen, waarbij vooraf

toestemming gegeven moet worden alvorens met sommige verwerkingsactiviteiten te kunnen starten. Het is daarbij wenselijk om de Rijksoverheid en de medeoverheden onder dezelfde centrale toezichthouder te laten vallen.

Belangrijke randvoorwaarden zijn dat de toezichthouder toegang heeft tot dat waar hij/zij toezicht op moet houden. Dat betekent dat de toezichthouder dezelfde beveiligingsmaatregelen moet nemen en dezelfde autorisaties moet hebben als de onder toezicht gestelde organisaties waar toezicht op Nationale Belangen betreft.

6. Conclusies en aanbevelingen

6.1. Het belang van Nationale Belangen

In het kader van de voorbereiding van wetgeving waarin een gemeenschappelijke wettelijke grondslag voor de omgang met en het toezicht op informatieveiligheid wordt geregeld, is de volgende onderzoeksvraag gesteld: *Hoe moet worden omgegaan met de belangrijkste/gevoeligste overheidsprocessen en -informatie?*

Complexe maatschappelijke opgaven vragen steeds vaker om samenwerking in ketens en netwerken, waarin gegevens gezamenlijk worden gebruikt. Daartoe zal steeds vaker gegevens bij de bron worden bewaard en uitsluitend daar bevraagd kunnen worden, in plaats van die gegevens steeds te verstrekken aan partijen die deze willen gebruiken in hun proces. Doordat dezelfde gegevens vervolgens een rol (kunnen) spelen in verschillende processen is het zaak dat deze adequaat beveiligd worden. Tegelijk verlangen burgers en bedrijven van de overheid betrouwbare informatie en betrouwbare dienstverlening. Daarvoor zijn betrouwbare, beschikbare en integere gegevens, documenten en registraties nodig. Voor de overheid is het van belang te weten over welke gegevens, documenten en registraties ze beschikt en deze duurzaam toegankelijk te houden en te beveiligen zodat betrouwbaarheid, integriteit en beschikbaarheid worden gegarandeerd.

Sommige gegevens (al dan niet vastgelegd in documenten, en de registraties die gegevens en/of documenten bevatten) zijn van groter belang dan andere. Een beperkt aantal gegevens, documenten en registraties is voor overheid en maatschappij van zodanig belang dat ze als 'van Nationaal Belang' kunnen worden aangemerkt.

In dit onderzoek hebben we de volgende analogie gebruikt voor de digitale overheid: als duidelijk is wat de digitale 'kroonjuwelen' zijn die kunnen worden aangemerkt als 'van Nationaal Belang', dan kunnen aan organisaties, systemen en processen die gebruikmaken van die 'kroonjuwelen' eisen worden gesteld ten aanzien van beveiliging van deze digitale kroonjuwelen.

Deze analogie heeft als voordeel dat wordt aangesloten bij de ontwikkeling naar een federatief datastelsel en dat niet telkens hoeft te worden vastgesteld welke (delen van) veranderlijke processen en systemen van Nationaal Belang moeten worden verklaard. Verwerking van deze gegevens en documenten (soms uit registraties) is mogelijk voor alle overheden, mits ze (en hun systemen) aan de vastgestelde eisen voldoen.

6.2. Afwegen van belangen

Er bestaat geen universele methode voor het afwegen van belangen. Ook wanneer gekeken wordt naar de methoden en werkwijzen voor het definiëren of afwegen van belangen binnen de overheid komt dit in de meeste gevallen neer op: "van belang is wat de organisatie van belang vindt". Dat gaat in veel gevallen in meer of mindere mate voorbij aan het waarde die buiten de organisatie kan worden gehecht aan specifieke belangen, zeker wanneer het gaat om gegevens, documenten en registraties die in toenemende mate éénmaal worden gemaakt en vervolgens worden (her)gebruikt door verschillende organisaties, overheidsorganisaties op alle lagen én organisaties en personen buiten de overheid, bovendien in geheel verschillende processen.

Dit onderzoek beoogt bij te dragen aan het ontwikkelen van een *generiek gemeenschappelijk kader* voor het kunnen bepalen welke gegevens, documenten en registraties kunnen worden aangemerkt als van Nationaal belang. Daarmee wil

dit onderzoek belangen identificeren die naar hun *aard* belangrijk zijn, een *intrinsieke waarde* hebben en een zeker mate van onveranderlijkheid hebben. Door aan te sluiten bij intrinsiek belang in plaats van een afweging van belang, dreiging en weerstand (risicobenadering) én door te benadrukken dat het ziet op relatief onveranderlijke, herkenbare entiteiten waarvan het belang dat van een individuele overheidsorganisatie en -laag en zelfs dat van de gehele overheid overstijgt, komen we tot de volgende criteria:

Criteria voor gegevens, documenten en registraties van Nationaal Belang:

- Het betreft op zichzelf staande informatie-elementen of -objecten van de overheid: gegevens, documenten en registraties;
- Deze gegevens, documenten en registraties hebben een grote mate van onveranderlijkheid (wat niet geldt voor processen en systemen);
- Gegevens, documenten en registraties van Nationaal Belang hebben een intrinsiek belang voor meerdere of alle overheidsorganisaties, voor veel of alle burgers en bedrijven, en/of zelfs voor de gehele Staat. Vanwege hun uniciteit, authenticiteit, vertrouwelijkheid, beschikbaarheid of een combinatie van die aspecten vormen ze een cruciaal element in het betrouwbaar en rechtmatig kunnen handelen van de Nederlandse Staat en/of de Nederlands overheid en/of grote delen van de maatschappij. In geval van compromitteren, of de mogelijkheid van compromitteren kan grote schade ontstaan voor de Staat, voor zijn bondgenoten en/of voor grote delen van de maatschappij.

Op basis van deze criteria kunnen de volgende categorieën gegevens, documenten en registraties worden onderscheiden:

- **Bijzondere (gerubriceerde) informatie**
  Alle bijzondere (gerubriceerde) informatie die valt onder het VIRBI 2013, of onder een internationaal verdrag of overeenkomst (van tenminste het niveau Stg.GEHEIM) en gegevens die zijn opgeslagen in een verboden plaats. Omdat een rubricering cf. het VIRBI 2013 moet worden “aangebracht op informatie” betreft dit veelal documenten.
- **Nationale Basisregistraties**
  Alle nationale (basis)registraties - waaronder in elk geval alle basisregistraties – met een wettelijke basis, die cruciale, authentieke gegevens en/of documenten bevatten over personen, organisaties, gebouwen, geografie en economie. Ook de registraties met koppelgegevens, die gegevens van de ene registratie aan gegevens van een andere registratie koppelen, vallen hieronder als het om een koppeling met een registratie van Nationaal Belang gaat. Hierbij zijn ook de voorzieningen om deze registraties te raadplegen belangrijk. Deze voorzieningen (met een wettelijke basis) die gegevens raadplegen die van Nationaal Belang moeten ook voldoen aan een aantal vereisten.
- **Overige (documenten en) registraties van Nationaal Belang**
  Andere (documenten en) registraties kunnen volgens een systematiek identiek aan het afwegen van belangen van het Nationaal Archief ten aanzien van selectielijsten worden voorgedragen om ook te worden vastgesteld als Nationaal Belang.
- **Overige gegevens, documenten en registraties (al dan niet tijdelijk) op basis van een politieke belangenafweging**
  Naar aanleiding van een *politieke* belangenafweging kunnen overige gegevens, registraties, en documenten van de overheid die door de Minister van BZK (ook tijdelijk) tot ‘Nationaal Belang’ worden verklaard. Dit heeft gelijkenis met de zgn. hotspot-monitor, alleen zullen hier andere criteria moeten worden aangelegd.

6.3. Het vaststellen van Nationale Belangen

Het vaststellen van welke gegevens, documenten en registraties worden aangemerkt als van Nationaal Belang geschiedt door de minister of staatsecretaris van het vakdepartement die het betreft met de Minister van BZK samen. De Minister van BZK stelt bovendien vast *dat* gerubriceerde documenten vanaf een bepaald rubriceringsniveau als Nationaal Belang worden aangemerkt én *wat* vervolgens de eisen zijn aan verwerken, verwerkers, systemen, locaties, etc.
Maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang

Ten aanzien van de maatregelen wordt aangesloten bij het VIRBI 2013, waardoor eisen gelden en maatregelen kunnen worden getroffen als aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007) en het Beveiligingsvoorschrift Rijk 2013 (BVR 2013), die ook onverkort van toepassing zijn. Het VIRBI moet wel op enkele punten worden uitgebreid en aangepast om de reikwijdte uit te breiden naar – naast de Rijksoverheid - andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties – het zal dan mogelijk een andere vorm (wet) krijgen. Ook moet het VIRBI 2017 uitgebreid worden met centraal toezicht.

Verder worden maatregelen voorgesteld die zien op standaarden, verplicht gebruik van overheidsvoorzieningen en aanbestedingen van ICT-diensten en ICT-producten:

Concrete maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang

- Gegevens, documenten en registraties van Nationaal Belang worden aangemerkt als bijzondere informatie: informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries, zoals gedefinieerd in het VIRBI 2013. Het VIRBI dient op enkele punten te worden aangepast en uitgebreid.
- Alle ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen gelden de (open) standaarden van de 'Pas toe of leg uit-lijst', afwijken kan alleen na expliciete toestemming.
- Uitwisseling van gegevens van Nationaal Belang verloopt verplicht via Diginetwerk, Digipoort en Digikoppeling
- Identificatie en authenticaties voor raadplegen van gegevens verloopt verplicht via DigiD.
- Voor aanbesteding van ICT-diensten en ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kunnen uitzonderingen op de Aanbestedingswet en de Aanbestedingswet op defensie- en veiligheidsgebied worden ingezet.

Daarnaast is nog een aantal concrete maatregelen voorstelbaar waarvan de mogelijkheid, wenselijkheid en haalbaarheid nader onderzoek vereist:

Aanbevelingen voor nader onderzoek naar concrete maatregelen ten aanzien van gegevens, documenten en registraties van Nationaal Belang

- Onderzoek of het mogelijk en wenselijk is om specifieke locaties, zoals datacenters, aan te kunnen wijzen als verboden plaats.
- Onderzoek hoe bij ontwikkelen of aankopen van om ICT-diensten en ICT-producten ten behoeve van opslag, verwerking en uitwisseling van gegevens van Nationaal Belang kan worden meegewogen hoe de afhankelijkheid van niet-Europese producten en diensten kan worden beperkt en verplicht mogelijkheden daartoe in aanbestedingen.
- Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht gebruik moeten maken van/ bestaan uit door het NBV geëvalueerde producten.
- Onderzoek of ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen verplicht moeten worden ontwikkeld via een proces van Secure Software Development.
- Onderzoek hoe voor ICT-producten om opslag, verwerking en uitwisseling van gegevens van Nationaal Belang digitaal te doen verlopen kan worden aangesloten op de ontwikkelingen in de Nationale Cryptostrategie.

Er dient nog wel een impactanalyse gemaakt te worden om te onderzoeken of de voorgestelde maatregelen in verhouding staan tot de gewenste niveaus van beveiliging en kwaliteitseisen enerzijds, en de werkbaarheid anderzijds.

6.4. Het vaststellen van Nationale Belangen

De reikwijdte van het belang van deze digitale kroonjuwelen voor de overheid en voor de maatschappij maakt bovendien dat centraal, nationaal toezicht noodzakelijk is om tot een adequaat en uniform niveau van beschikbaarheid, vertrouwelijkheid en integriteit van de gegevens, documenten en registraties van Nationaal Belang te komen. Dat toezicht strekt over de Rijksoverheid en over andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties. Het toezicht strekt zich bovendien ook uit over de overheidsvoorzieningen die verplicht moeten worden gebruikt (ook voor het deel waarbij deze voorzieningen worden aangewend voor toegang of uitwisseling van andere gegevens dan gegevens van Nationaal Belang).

Voor toezicht op gegevens, documenten en registraties van Nationaal Belang zou het toezicht kunnen worden ingericht vergelijkbaar met het toezicht op de beveiliging van gerubriceerde informatie van EU en NAVO. Daarbij wordt ingezet op een initiële accreditatie van de betreffende beveiliging bij de overheidspartijen *vóóraf*, aangevuld door periodieke inspecties.

6.5. Tot slot

Bij de start van dit onderzoek is geprobeerd zicht te krijgen op 'informatiebeveiliging' en wat dan beveiligd zou moeten worden: gegevens, informatie, documenten, archiefbescheiden, datasets, registraties, processen, systemen, enzovoorts. Er is een grote diversiteit aan begrippen waarmee elementen van de informatiehuishouding en informatiebeveiliging binnen de overheid wordt aangeduid. Die begrippen worden bovendien in verschillende wet- en regelgeving op verschillende wijze gebruikt of uitgewerkt. Gelet op het belang van gegevens in de huidige tijd zou het goed zijn dat er uniforme definities komen van verschillende begrippen en dat deze op een even uniforme wijze worden toegepast in wet- en regelgeving, maar ook in het dagelijks gebruik binnen de overheid.

TwynstraGudde

Bijlagen

Bijlage 1: Wat te beschermen? – de veelheid aan begrippen

De overheid produceert, ontvangt en bewaart gegevens, informatie en documenten. Maar voor *gegevens*, *informatie* en *documenten*, de verwerking hiervan – inclusief bewaren of vernietigen - door de overheid (wat 'verwerking' inhoudt wordt hieronder ook besproken) en de processen en systemen waarin die verwerking plaatsvindt worden verschillende definities gebruikt in wet- en regelgeving. In deze bijlage worden verschillende begrippen – en daarbij is geen volledigheid nagestreefd, maar de selectie geeft al een goede indruk van de problematiek - nader geduid. Voor de definities wordt aangesloten bij bestaande (en soms aanstaande) wet- en regelgeving en bij door de Rijksoverheid vastgestelde kaders. Tegelijk kan worden vastgesteld dat soms dezelfde begrippen op verschillende plaatsen verschillend worden gedefinieerd.

Gegevens en informatie

Gegevens zijn de weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat.[116] Gegevens zijn de objectief waarneembare neerslag of registratie van feiten op een bepaald medium, zodanig dat deze gegevens uitgewisseld en voor langere tijd bewaard kunnen worden. Het betreft hier alle vormen van gegevens, zowel gegevens uit informatiesystemen als records en documenten, in alle vormen zoals gestructureerd als ongestructureerd. Met deze gegevens wordt een model (een selectief deel dus) van de werkelijkheid vastgelegd in de tijd. Ofschoon de werkelijkheid nooit stilstaat, kan deze door het vastleggen van de gegevens toch worden bevroren.

Met **informatie** worden betekenisvolle gegevens aangeduid.[117] Een gegeven zonder duidelijkheid over het type gegeven (bijvoorbeeld naam, geslacht e.d.) biedt geen informatie. Het gegeven '21' betreffende een persoon biedt zonder nadere context geen duidelijkheid – het kan gaan om leeftijd, gewicht of een ander aspect van een persoon. De waarden 'Jan' en 'man' zijn betekenisvolle gegevens betreffende de naam en het geslacht van een object van het type Persoon. Bij dergelijke betekenisvolle gegevens spreekt men niet meer van gegevens maar van informatie. Het Nationaal Archief spreekt van een **informatieobject**: "Een op zichzelf staand geheel van gegevens met een eigen identiteit".[118] Een 'eigen identiteit' betekent hier dat een informatieobject een naam of identiteitskenmerk heeft waardoor het te onderscheiden is van andere informatieobjecten. Wanneer een informatieobject uit meerdere informatieobjecten bestaat, dan wordt gesproken over een **aggregatie**. Een informatieobject kan vastgelegd zijn als bestand of in een gegevensbase en kan verspreid zijn over diverse fysieke locaties.

De begrippen gegeven en informatie lopen in definities in diverse wetgeving nogal eens door elkaar. Gegevens bestaan onder de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv2017) uit persoonsgegevens en andere gegevens. Volgens de Wiv2017 zijn **persoonsgegevens** gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individueel natuurlijke persoon. Daarmee zijn het betekenisvolle gegevens, dus informatie. De Algemene verordening gegevensbescherming (AVG) ziet feitelijk ook alleen op betekenisvolle (persoons)gegevens: een **persoonsgegeven** is volgens de AVG alle *informatie* over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Voor de hand liggende

[116] De definities van gegeven en informatie zijn overgenomen van de Nederlandse Overheid Referentie Architectuur (NORA). NORA bevat principes, beschrijvingen, modellen en standaarden voor het ontwerp en de inrichting van de overheid. Het is een instrument dat door overheidsorganisaties kan worden benut in de verbetering van de dienstverlening aan burgers en bedrijven en is in 2008 door het Kabinet vastgesteld als norm voor alle overheidsorganisaties.
[117] Bron: NEN-ISO 9000.
[118] Informatieobject | Nationaal Archief.

persoonsgegevens zijn iemands naam, adres en woonplaats, maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Er kan ook sprake zijn van **indirecte persoonsgegevens**. Het gaat dan om gegevens die in combinatie met andere gegevens iets zeggen over een persoon (tot een persoon herleidbaar zijn). Daarnaast onderscheidt de AVG **bijzondere persoonsgegevens**: gevoelige gegevens als iemands ras, godsdienst of gezondheid. Deze zijn door de wetgever extra beschermd.[119]

Een **database**, gegevensbank of databank is een (meestal digitaal opgeslagen) gegevensverzameling, ingericht met het oog op flexibele raadpleging en gebruik. Een **gegevensbank** is een verzameling van werken, gegevens of andere zelfstandige elementen die systematisch of methodisch geordend en afzonderlijk met elektronische middelen of anderszins toegankelijk zijn en waarvan de verkrijging, de controle of de presentatie van de inhoud in kwalitatief of kwantitatief opzicht getuigt van een substantiële investering.[120] Deze gegevensbanken kunnen in bezit zijn van private ondernemingen, maar bijvoorbeeld ook van (wetenschappelijke) onderzoeksinstellingen, universiteiten, voor het publiek toegankelijke bibliotheken, voor het publiek toegankelijke musea, archieven of instellingen voor cinematografisch of audio(visueel) erfgoed. De inhoud van deze gegevensbanken kan geheel of gedeeltelijk aan het publiek ter beschikking worden gesteld.

Gegevens van de overheid worden proactief beschikbaar gesteld, indien geen uitzonderings- of beperkingsgronden van de Wet openbaarheid van bestuur of bijzondere openbaarmakingsregelingen van toepassing zijn.[121] Het gegevensbankenrecht beschermt tegen het opvragen of hergebruiken van een groot deel van de gegevens (de gegevens) in de gegevensbank. Naast de Nederlandse Gegevensbankwet, is er ook een Europese Richtlijn voor de rechtsbescherming van gegevensbanken.[122]

Registraties zijn databronnen met een wettelijke grondslag. Overheidsorganisaties hebben een wettelijke taak om bepaalde gegevens te verzamelen en te registeren in zogenaamde **registraties**. Veel overheidsorganisaties hebben een taak om voor een specifiek domein of sector de registraties te beheren. Er zijn ruim honderdvijftig sectorregistraties geïdentificeerd[123], die wettelijk door of in opdracht van overheidsorganisaties worden bijgehouden. In het domein *Rechtspraak* bijvoorbeeld betreft dit het Boedelregister, het Centraal Curatele- en Bewind register, het Centraal Testamentenregister, het Huwelijksgoederenregister, het Landelijk Register Schuldsanering, het Landelijk Uniform Registratiesysteem Internationale Rechtshulp, het Nederlands Register Gerechtelijk Deskundigen, het Register beëdigde tolken en vertalers, het Register notariaat en de Registratie Advocaten.

Een aantal registraties van de overheid is aangewezen als **Nationale Basisregistratie**. Een basisregistratie is een door de overheid officieel aangewezen registratie met daarin gegevens van hoogwaardige kwaliteit, zogenaamde **basisgegevens**, die door alle overheidsinstellingen verplicht en zonder nader onderzoek, worden gebruikt bij de uitvoering van publiekrechtelijke taken. De kenmerken van een basisregistratie zijn verwoord in specifieke eisen[124] waaraan een basisregistratie moet voldoen. Basisregistraties bevatten *authentieke en niet-authentieke gegevens*. Een authentiek gegeven is een in een basisregistratie opgenomen gegeven dat bij wettelijk voorschrift als authentiek is aangemerkt. Het verplicht gebruik door overheidsinstellingen geldt voor de authentieke gegevens in een basisregistratie. In de wet van een basisregistratie ligt vast welke gegevens authentiek zijn.

[119] Voor meer informatie zie: Wat zijn persoonsgegevens?
[120] Gegevensbankwet (2021).
[121] Zie bijvoorbeeld het gegevensregister op Gegevensregister van de Nederlandse Overheid | Gegevens overheid
[122] Zie voor meer informatie: EUR-Lex - 31996L0009 - EN - EUR-Lex (europa.eu)
[123] Voor meer informatie zie: Sectorregistraties.
[124] Voor meer informatie zie: Overzicht van alle onderwerpen, stelsel van 12 basisregistraties.

Informatie, registraties en documenten binnen de overheid

Er zijn veel verschillende soorten informatie die de overheid verwerkt (over verwerken: zie volgende paragraaf). Een aantal voorbeelden (niet limitatief):

- informatie over personen, organisaties en objecten (gebouwen, voertuigen, etc.);
- informatie als onderdeel van een processtap, zoals een ingevulde vergunningaanvraag, een bestelling of een klacht;
- informatie die de overheid produceert als uitvloeisel van processen, zoals beleidsstukken, wetgeving, onderzoeken en vergunningen;
- informatie over het functioneren van de overheid, zoals dienstbeschrijvingen, leveringsvoorwaarden en rapportages.

Deze informatie kan onder meer aangeduid worden naar inhoud of context, naar status en naar gedaante. In elk geval onderscheidt de wetgever ten aanzien van overheidsinformatie in elk geval *bijzondere informatie*, *basisgegevens, documenten* en gegevens in *gegevensbanken*.

Bijzondere informatie

Informatie wordt **bijzondere informatie** waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries.[125] Informatie waarvan de geheimhouding vanwege het belang van de Staat, zijn bondgenoten of van één of meer ministeries daarom is geboden, moet worden voorzien van een passend niveau van rubricering. Dit rubriceringsniveau is een aanduiding van de verwachte nadelige gevolgen aan de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries zijn als (een deel van) de informatie bekend wordt bij niet geautoriseerden. Nederland kent 4 niveaus van rubricering van bijzondere informatie binnen de overheid[126]:

- Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG) - indien kennisname door niet geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten;
- Staatsgeheim GEHEIM (afgekort Stg.G) - indien kennisname door niet geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten;
- Staatsgeheim CONFIDENTIEEL (afgekort Stg.C) - indien kennisname door niet geautoriseerden schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten;
- Departementaal VERTROUWELIJK (afgekort Dep.V.) - indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.

Overigens kan een overheidsorganisatie ook bijzondere informatie verkrijgen krachtens een internationaal verdrag of overeenkomst, bijvoorbeeld in het kader van het Nederlands lidmaatschap van de EU of de NAVO.[127] Deze informatie kan dan al bij ontvangst of opmaak een andere rubricering krijgen, conform de binnen die internationale verdragen of overeenkomsten gelden afspraken.

Tot slot zijn er gegevens waarvan de geheimhouding door het belang van de veiligheid van de staat (en diens bondgenoten) wordt geboden.[128] Elke plaats in gebruik bij de staat of bij een staatsbedrijf *kan* ter bescherming van dergelijke gegevens worden aangewezen als *verboden plaats*. En wanneer buitengewone omstandigheden dit noodzakelijk maken kan bij Koninklijk Besluit, op voordracht van de Minister-President, elk werk van openbaar verkeer

[125] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).
[126] Handleiding Rubricering, 2015.
[127] Zie bijvoorbeeld: NAVO: "Security within the North Atlantic Treaty Organisation", AC/35-D/2000 t/m 2005, C-M(2002)49 EC: Council Security Rules) en C-M(2002)50.
[128] Wet bescherming staatsgeheimen (2013).

en elk werk van openbaar nut ter bescherming van gegevens, waarvan op dat moment de geheimhouding door het belang van de veiligheid van de staat (en diens bondgenoten) wordt geboden, als verboden plaats worden aangewezen. Om welke gegevens dit gaat of zou kunnen gaan en wie bepaalt welke gegevens dit betreft wordt niet nader aangeduid, maar doordat de wet waarin deze mogelijkheden zijn vastgelegd de titel *Wet bescherming staatsgeheimen* draagt lijkt een link naar gerubriceerde informatie voor de hand te liggen.

Documenten van de overheid

Gegevens en vooral informatie worden vaak vastgelegd in documenten, of beter: een **informatieobject**[129], wat een op zichzelf staand geheel van gegevens met een eigen identiteit is. Voorbeelden van informatieobjecten/documenten zijn brief, e-mail, video, webpagina, tweet, subsidieaanvraag, vergunning. Een **document** in de context van de overheid is – volgens de Archiefwet 1995[130] - een schriftelijk stuk of ander geheel van vastgelegde gegevens. De Archiefwet sluit aan bij de Wet open overheid[131] waarin een document in de context van de overheid is gedefinieerd als een door een orgaan, persoon of college (als bedoeld in artikel 2.2, eerste lid van de Woo) opgemaakt of ontvangen *schriftelijk stuk of ander geheel* van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college. Met 'een schriftelijk stuk of ander geheel van vastgelegde gegevens' beoogt de wetgever een ruime en techniek neutrale uitleg: in beide gevallen is de precieze drager waarop gegevens zijn vastgelegd in wezen niet van belang voor de vraag of van documenten kan worden gesproken.[132] In de Wet hergebruik van overheidsinformatie wordt een document gedefinieerd als een bij een met een publieke taak belaste instelling berustend *schriftelijk stuk of ander materiaal dat gegevens bevat*.[133]

Documenten vallen ook onder bovengenoemde informatieobjecten en wanneer deze documenten vallen onder de Archiefwet 1995 dan wordt gesproken over **archiefbescheiden**.[134] Bij archiefbescheiden gaat het dus om informatie gebonden aan de werkprocessen van het overheidsorgaan. De wet omschrijft archiefbescheiden als

1. *bescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten;*
2. *bescheiden, ongeacht hun vorm, met overeenkomstige bestemming, ontvangen of opgemaakt door instellingen of personen, wier rechten of functies op enig overheidsorgaan zijn overgegaan;*
3. *bescheiden, ongeacht hun vorm, welke ingevolge overeenkomsten met of beschikkingen van instellingen of personen dan wel uit anderen hoofde in een archiefbewaarplaats zijn opgenomen om daar te berusten;*
4. *reproducties, ongeacht hun vorm, welke bij of krachtens de wet in de plaats zijn gesteld van de onder 1°, 2° of 3° bedoelde archiefbescheiden of welke op grond van het bepaalde in artikel 7 zijn vervaardigd.*[135]

De woorden "naar hun aard" geven aan dat een overheidsorgaan een informatieobject niet naar eigen goeddunken kan bestempelen tot wel of geen archiefstuk want het bronproces van het informatieobject bepaalt of het een archiefstuk is of niet.

[129] Zie: Informatieobject..
[130] Archiefwet (1995).
[131] Wet van 25 oktober 2021 tot wijziging van het voorstel van wet van de leden Snels en Sneller houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid 2022)
[132] Memorie van toelichting bij Voorstel van Wet tot intrekking van de Archiefwet 1995 en vervanging door de Archiefwet 2021 (Archiefwet 2021).
[133] Wet hergebruik van overheidsinformatie (2015).
[134] Archiefbescheiden | Nationaal Archief
[135] Archiefbescheiden | Nationaal Archief

Verwerking van gegevens en informatie

Gegevens en informatie kunnen worden verwerkt. **Verwerken** is een zeer ruim begrip. Handelingen die er volgens de Algemene verordening gegevensbescherming (AVG) in ieder geval onder vallen, zijn: het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, en het wissen en vernietigen van gegevens.[136] De AVG[137] voegt hier nog aan toe dat het bij gegevensverwerking kan gaan om "een bewerking of een geheel van bewerkingen met betrekking tot (persoons)gegevens of een geheel van (persoons)gegevens" en dat de uitvoering van de bewerking al dan niet via geautomatiseerde procedés kan verlopen.

Informatiesystemen en informatiehuishouding

Verwerking van gegevens vindt plaats binnen een informatiesysteem. Een **informatiesysteem** is volgens het VIR een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.[138] Een informatiesysteem is in deze zin dus niet hetzelfde als een computersysteem: een computersysteem kan een element zijn van het informatiesysteem. Maar ook processen en personen zijn volgens de VIR-BI-definitie een onderdeel van een informatiesysteem.

In de Wbni[139] wordt voor de definitie van netwerk- en informatiesysteem verwezen naar de NIS-richtlijn[140], waarin staat de definitie luidt van "netwerk- en informatiesysteem":

a) een elektronisch communicatienetwerk (de transmissiesystemen en in voorkomend geval de schakel- of routeringsapparatuur en andere middelen die het mogelijk maken signalen over te brengen via draad, radiogolven, optische of andere elektromagnetische middelen waaronder satellietnetwerken, vaste (circuit- en pakket geschakelde, met inbegrip van internet) en mobiele terrestrische netwerken, elektriciteitsnetten, voor zover deze voor overdracht van signalen worden gebruikt, netwerken voor radio- en televisieomroep en kabeltelevisienetwerken, ongeacht de aard van de overgebrachte informatie);
b) een apparaat of groep van geïnterconnecteerde of bij elkaar behorende apparaten, waarvan een of meer, overeenkomstig een programma, digitale gegevens automatisch verwerkt of verwerken, of
c) digitale gegevens die via in de punten a) en b) bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan.

Deze definitie ligt dichter bij wat in het spraakgebruik wordt aangeduid als informatiesysteem.

De Rijksoverheid zelf gebruikt veelvuldig de term informatiehuishouding om het totaal van opslag, beheer en verstrekking van gegevens binnen een organisatie aan te duiden.[141] Of, specifieker gedefinieerd[142]: **Informatiehuishouding** is het totaal aan regels, voorzieningen, activiteiten en processen gericht op de

[136] Zie voor meer informatie: Wat houdt verwerken van persoonsgegevens in?
[137] Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming, 2018: 24.
[138] Besluit voorschrift informatiebeveiliging rijksdienst 2007.
[139] Wet beveiliging netwerk- en informatiesystemen (2018).
[140] Richtlijn (EU) 2016/1146 - Cyberbeveiliging van netwerk- en informatiesystemen. van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.
[141] NORA geeft als definitie: "Het totaal aan regels en voorzieningen gericht op de informatiestromen en –opslag of archivering ter ondersteuning van de primaire processen."
[142] Rijksprogramma Duurzaam Digitale Informatiehuishouding, 2021. Open op Orde Generiek actieplan informatiehuishouding Rijksoverheid.

informatiestromen en op het beheer van informatie.[143] De informatiehuishouding ondersteunt de primaire processen van overheidsorganisaties en waarborgt *democratische, juridische en historische waarden*. Om dat tweeledige doel van ondersteunen en waarborgen te bereiken moet een informatiehuishouding zo worden ingericht dat (digitale) informatie die nodig is om het handelen van overheidsorganisaties te kunnen reconstrueren van meet af aan, maar ook na verloop van tijd duurzaam toegankelijk is en blijft. **Duurzaam toegankelijk** betekent vindbaar, beschikbaar, leesbaar, interpreteerbaar en betrouwbaar voor degenen die er recht op hebben, vanaf het moment van ontstaan en voor zo lang als noodzakelijk. Hierbij wordt rekening gehouden met aspecten van openbaarheid en privacy. Duurzaam betekent dat de toegankelijkheid van de informatie bestand is tegen veranderingen van elke aard. Dit is niet alleen nodig voor de informatie die binnen de werkprocessen verwerkt wordt, maar ook van de contextinformatie (zoals wie, wat, waarom, waar, etc.). Duurzaam toegankelijk geldt vanaf het moment van creatie tot het moment dat de informatie niet meer nodig is, ook niet als cultureel erfgoed.[144]

Onderdeel van deze informatiehuishouding is de **koppeling van systemen** tussen overheden en de koppeling met systemen buiten de overheden. DigiD is een voorbeeld van een systeem wat geraadpleegd mag worden door organisaties die een publieke wettelijk vastgestelde taak uitvoeren waarbij zij het Burgerservicenummer of A-nummer mogen gebruiken. Er worden eisen gesteld aan organisaties die een koppeling mogen maken met het DigiD-systeem, zo moeten organisaties voldoen aan een beveiligingsnorm.[145] Er zijn naast systemen ook andere plekken waar gegevensuitwisseling met de overheid plaatsvindt, denk hierbij aan email of via websites. Hierbij moeten burgers en ondernemers erop vertrouwen dat **gegevensuitwisseling** met de overheid veilig verloopt, hiervoor moeten overheden diverse **informatieveiligheidsstandaarden** toepassen. Opvallend is dat hier de begrippen 'gegeven' en 'informatie' als synoniem worden gebruikt, en ziet de standaard volgens de naam op 'beveiliging van informatie' maar gaan de maatregelen vooral over beveiliging van een 'netwerk- en informatie*systeem*'. Onder de koppeling van systemen liggen vaak '**afsprakenstelsels'**. Dit zijn nauwe samenwerkingsvormen van verschillende partijen uit het bedrijfsleven, de overheid en de wetenschap, die producten of diensten leveren, op basis van vastgelegde eisen. Een afsprakenstelsel bevat de spelregels voor leveranciers en gebruikers met een kwaliteitsgarantie.

In het Generiek Actieplan Informatiehuishouding Rijksoverheid worden informatiesystemen gezien als één (van drie, naast *professionals informatiebeheer* en *aard en volume van informatie*) van de aspecten gezien van een informatiehuishouding (zie Figuur 7):

Figuur 7: Illustratie met als titel 'Drie samenhangende aspecten van de informatiehuishouding'. Uit Open op Orde. Generiek Actieplan Informatiehuishouding Rijksoverheid

[143] Opvallend is dat in deze definitie verwijzingen naar zowel personen als de gegevens of informatie zelf ontbreken (hoewel deze later wel weer als aspect worden benoemd – zie verderop), terwijl deze de NORA-definitie van informatiesysteem juist start met "samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen …".
[144] Ibidem.
[145] ICT-beveiligingsassessments DigiD.

Over informatiesystemen wordt in het Actieplan het volgende gezegd: "*Informatiesystemen* ondersteunen de organisaties en medewerkers optimaal bij hun *informatiehuishouding* en hun werkprocessen. Het IT-landschap[146] bij het Rijk is duurzaam toegankelijk, voldoet aan de kwaliteitseisen, is gebruiksvriendelijk en interoperabel. Er is sprake van hoge kwaliteit met zoveel mogelijk uniformiteit en standaardisatie.[147] Bij nieuwe en aangepaste informatiesystemen worden de maatregelen bepaald en uitgevoerd als onderdeel van de projecten waarin de systemen worden gekocht, gemaakt en ingericht (archivering by design)."[148]

Conclusie betreffende begrippen en definities

Niet alleen gegevens en informatie worden in verschillende wet- en regelgeving door elkaar gebruikt, dat geldt ook voor de begrippen registratie en document. Een document is een geheel van gegevens, wat dus in theorie ook een registratie zou kunnen zijn. Een registratie is een bestand van gegevens, maar zou heel goed ook een bestand van documenten kunnen zijn. En zowel een gegeven, een document als een registratie zou kunnen worden aangemerkt als bijzondere informatie (en bijvoorbeeld van een rubricering kunnen worden voorzien). Dat laatste is voor het vervolg cruciaal, want daarmee kan dus een afweging gemaakt worden over *het belang* van zowel gegevens, informatie, documenten als registraties. Net als de begrippen 'gegevens', 'informatie', 'registratie' en 'document' worden ook 'informatiesysteem' en 'informatiehuishouding' naast en door elkaar gebruikt.

Ook de problematiek van beveiliging van gegevens, documenten en registraties (en processen, systemen en nog meer) zou erbij gebaat zijn dat in wet- en regelgeving én in het dagelijks gebruik uniforme, eenduidige en goed afgebakende begrippen en definities worden gebruikt.

[146] Een term die verder niet wordt gedefinieerd, maar die waarschijnlijk verwijst naar het totaal aan informatiesystemen. De vraag is dan wel meteen of deze zonder meer duurzaam toegankelijk moeten zijn – mogelijk niet altijd voor iedereen.
[147] Hoewel in deze beschrijving wordt verwezen naar het belang van standaardisatie wordt NORA nergens genoemd in Open op Orde: Generiek actieplan informatiehuishouding Rijksoverheid, noch worden de definities van NORA gebruikt.
[148] Open op orde: generiek actieplan informatiehuishouding Rijksoverheid, p. 20.

Bijlage 2: Interviewlijst

Tabel 1: Interviewlijst

Organisaties	Gesproken op
Klankbordgroep	27 september 2022 8 december 2022 14 maart 2023 16 tot 25 mei 2023: Gelegenheid tot schriftelijk feedback op conceptrapportage.
SZW (onderdeel van de klankbordgroep)	29 september 2022
Rijksinspectie Digitale Infrastructuur (onderdeel van de klankbordgroep)	11 oktober 2022
Provincie Groningen (onderdeel van de klankbordgroep)	6 oktober 2022
BZK (onderdeel van de klankbordgroep)	3 oktober 2022
AIVD (onderdeel van de klankbordgroep)	19 oktober 2022
Ministerie van Financiën (onderdeel van de klankbordgroep)	20 oktober 2022
Nationaal coördinator Terrorismebestrijding en Veiligheid (NCTV)	20 oktober 2022
NOREA	19 oktober 2022
SSC ICT CISO	20 oktober 2022
VNG	9 november 2022
CIP	10 oktober 2022
Rijksinspectie Digitale Infrastructuur	17 oktober 2022
Forum Standaardisatie	19 oktober 2022
De Waag Future Lab	8 november 2022
NCSC	14 november 2022
BZK - Dossierhouder DigiD	14 november 2022
Adviescollege ICT	15 november 2022
I&W	16 november 2022
Logius	21 + 22 november 2022
BZK - Programmamanager basisregistraties	29 november 2022
BZK – Digitale overheid	30 november 2022
Beveiligingsautoriteit, hoofd bureau BVA voor JenV en BZK	22 december 2023
Inspectie Overheidsinformatie en Erfgoed – Hoofdinspecteur en plv. directeur	19 januari 2023
Inspectie overheidsinformatie en archief	17 maart 2023
BZK – Adviseur Informatiebeveiliging	5 april 2023

Bijlage 3: Bronnen

Adviescollege ICT-toetsing (2023). *Definitief Advies Logius ICT-infrastructuur.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/brieven/2023/04/12/definitief-advies-logius-ict-infrastructuur

Cybersecurity Raad (2021). *Nederlandse strategische autonomie en cybersecurity 2021*.

Interbestuurlijke Datastrategie (2023). Meerjarenaanpak Interbestuurlijke Datastrategie. Geraadpleegd van Onderzoeksrapport 'Nederlandse strategische autonomie en cybersecurity' | Rapport | Cyber Security Raad

Informatiebeveiliging Rijksdienst (2015). *Handleiding Rubricering.* Geraadpleegd van https://zoek.officielebekendmakingen.nl/blg-882736.pdf

Inspectie Justitie en Veiligheid (2022). *Samenhangend inspectiebeeld cybersecurity vitale processen 2021-2022* Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2022/07/06/tk-bijlage-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-21-22

Inspectie Overheidsinformatie en Erfgoed (2007). *Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR)* Geraadpleegd van https://www.inspectie-oe.nl/toezichtvelden/overheidsinformatie/wet--en-regelgeving/overige-informatiewetgeving/besluit-voorschrift-informatiebeveiliging-rijksdienst-2007

Inspectie Overheidsinformatie en Erfgoed (2023). *Werkprogramma 2023-2024 Toezicht op informatiehuishouding en digitalisering, omgang met het erfgoed.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2023/01/27/werkprogramma-2023-2024-inspectie-overheidsinformatie-en-erfgoed

Ministerie van Algemene Zaken (2023). *Veiligheidsstrategie voor het Koninkrijk der Nederlanden*. Geraadpleegd van https://www.rijksoverheid.nl/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2003). *Actieprogramma Elektronische Overheid.* Geraadpleegd van https://zoek.officielebekendmakingen.nl/kst-26387-18.html

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. (2020). *Integraal Afwegingskader Informatieveiligheid Overheid.* Geraadpleegd van http://www.kcbr.nl

Ministerie van Justitie en Veiligheid (2018). *Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming.* Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

Ministerie van Justitie en Veiligheid (2020). *Handleiding Algemene verordening gegevensbescherming (AVG)*. Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2018/01/22/handleiding-algemene-verordening-gegevensbescherming

Ministerie van Justitie en Veiligheid (2022). Nederlandse Cybersecuritystrategie 2022-2028. Ambities en acties voor een digitaal veilige samenleving. Geraadpleegd van https://open.overheid.nl/documenten/ronl-82f59d66894e136f786c3a34e62d1ce52d26b1c8/pdf

Nationaal Archief Ministerie van Onderwijs, Cultuur en Wetenschap (2015). *Belangen in Balans: Handreiking voor waardering en selectie van archiefbescheiden in de digitale tijd.* Geraadpleegd van https://www.nationaalarchief.nl/sites/default/files/field-file/Belangen%20in%20Balans_0.pdf

Nationaal Cyber Security Centrum (2023). *Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt.* Geraadpleegd van https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

NAVO (2002). *Security within the North Atlantic Treaty Organization.* Geraadpleegd van https://archives.nato.int/security-within-the-north-atlantic-treaty-organization

Noordbeek (2022). *Adviesrapport aangaande een Onderzoek voor een eenduidig afwegingskader Voor informatieveiligheidseisen vanuit Nationaal Belang.*
Geraadpleegd van https://open.overheid.nl/documenten/ronl-4590f723e423cccf576300e2446f6ec731be589f/pdf
Rijksdienst (2021). *Besluit BVA-stelsel Rijksdienst.*
Geraadpleegd van *https://www.rijksoverheid.nl/documenten/besluiten/2020/12/29/besluit-bva-stelsel-rijksdienst-2021*
Rijksoverheid (2013). *Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013.*
Geraadpleegd van *https://wetten.overheid.nl/BWBR0033507/2013-06-01*
Rijksoverheid (2015). *Leidraad: Te beschermen belangen.*
Rijksoverheid (2020). *Baseline Informatiebeveiliging Overheid.*
Geraadpleegd van *https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/kaders-voor-cybersecurity/baseline-informatiebeveiliging-overheid/*
Rijksoverheid (2021). Rijksprogramma Duurzaam Digitale Informatiehuidhouding. *Open op orde: generiek actieplan informatiehuishouding Rijksoverheid.*
Geraadpleegd van *https://www.rijksoverheid.nl/documenten/rapporten/2021/04/06/open-op-orde-generiek-actieplan-informatiehuishouding-rijksoverheid*
VKA (2019). *Onderzoek Toezicht en Verantwoording Informatieveiligheid Overheid Horizontaal en verticaal toezicht in balans.* Verdonck, Klooster & Associates B.V.
Geraadpleegd van https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2019/04/20190228-Onderzoeksrapport-toezicht-op-informatieveiligheid-BZK-Definitief-A-1.pdf
VKA (2020). *Onderzoek Vitale Infrastructuur in de Digitale Overheid: De Internationale praktijk van sturing en toezicht op vitale infrastructuren in de digitale overheid.*
Geraadpleegd van https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2020/03/VKA-20196563-BZK-Onderzoek-vitale-infrastructuur-in-de-digitale-overheid-v1.0-DT.pdf
VKA (2022). *Onderzoek toezicht op informatieveiligheid.*
Geraadpleegd van https://www.rijksoverheid.nl/documenten/rapporten/2022/03/04/onderzoek-toezicht-op-informatieveiligheid
Wetenschappelijke Raad voor het Regeringsbeleid (2019). Voorbereiden op digitale ontwrichting rapport nr. 101.
Geraadpleegd van https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Geraadpleegde wetgeving

Aanbestedingswet 2012.
Geraadpleegd van wetten.nl - Regeling - Aanbestedingswet 2012 - BWBR0032203(overheid.nl)
Aanbestedingswet op defensie- en veiligheidsgebied.
Geraadpleegd van wetten.nl - Regeling - Aanbestedingswet op defensie- en veiligheidsgebied - BWBR0032898 (overheid.nl)
Archiefwet 1995.
Geraadpleegd van https://wetten.overheid.nl/BWBR0007376/2022-05-01
Archiefwet 2021.
Geraadpleegd van https://wetgevingskalender.overheid.nl/Regeling/WGK007100
Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013).
Geraadpleegd van https://wetten.overheid.nl/BWBR0033507/2013-06-01

Gegevensbankwet 2021.
Geraadpleegd van https://wetten.overheid.nl/BWBR0010591/2021-06-07
Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners (2018).
Geraadpleegd van https://wetten.overheid.nl/BWBR0041515/2022-12-01
Richtlijn (EU) 2016/1146 - Cyberbeveiliging van netwerk- en informatiesystemen.
Geraadpleegd van https://eur-lex.europa.eu/legal-content/NL/LSU/?uri=CELEX:32016L1148
Uitvoeringswet Algemene verordening gegevensbescherming (2018).
Geraadpleegd van https://wetten.overheid.nl/BWBR0040940/2021-07-01
Wet bescherming staatsgeheimen 2013.
Geraadpleegd van https://wetten.overheid.nl/BWBR0040940/2021-07-01
Wet hergebruik van overheidsinformatie 2015.
Geraadpleegd van https://wetten.overheid.nl/BWBR0036795/2021-07- 01
Wet open overheid 2022.
Geraadpleegd van https://wetten.overheid.nl/BWBR0045754/2023-02-18

TwynstraGudde adviseert overheid en bedrijfsleven op veel van de grote en urgente thema's van deze tijd. Denk aan veiligheid, diversiteit, digitalisering, mobiliteit, duurzaamheid, energie, financiën en gezondheid. We bieden onze opdrachtgevers unieke, werkbare oplossingen en brengen complexe projecten en programma's tot een goed einde. Iets creëren van blijvende waarde, daar gaan we voor. Daardoor hebben we een directe impact op (toekomstige) maatschappelijke en economische ontwikkelingen. En dus een grote impact op morgen.

TwynstraGudde

Impact op morgen.