ONDERZOEK WETGEVINGSKADER INFORMATIEVEILIGHEID

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

ONDERZOEK WETGEVINGSKADER INFORMATIEVEILIGHEID

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Remy Carré (VKA)
Leonie Gerding (VKA)
Wubbo Wierenga (Berenschot)

DATUM	**15-3-2020**
STATUS	Definitief
VERSIE	1.0
PROJECTNUMMER	20196564
INTERNE TOETS	Dick Brandt (VKA) Rianne Zivali – de Kievit (Berenschot) Hans Reterink (Berenschot)

INHOUDSOPGAVE

Inhoudsopgave		**3**
1	**Inleiding**	**5**
1.1	Achtergrond en onderzoeksopdracht	5
1.2	Aanpak van het onderzoek	6
2	**Typologiën van informatieveiligheidsregels**	**9**
2.1	Inleiding	9
2.2	Drie categorieën van informatieveiligheidsregels	9
2.3	Vijf manieren om informatieveiligheidsregels te stellen	10
2.4	Conclusie typering informatieveiligheidsregels en regelgevingspatronen	15
3	**Belangrijke thema's voor informatieveiligheidsregels**	**17**
3.1	Introductie	17
3.2	Informatieveiligheidsregels in ketensamenwerkingen	17
3.3	Regels over toezicht, handhaving, verantwoording en governance	18
3.4	De relatie tussen wettelijke producteisen en informatieveiligheidsregels	19
3.5	Conclusie 3 drie belangrijke thema's voor informatieveiligheidsregels	20
4	**Praktijkobservaties over de doorwerking van informatieveiligheidsregels in de praktijk**	**21**
4.1	Praktijkobservatie I: hoe informatieveiligheidsregels ook zijn opgesteld, ze worden altijd vertaald naar processen en producten die de personen op de werkvloer helpen om compliant te zijn.	21
4.2	Praktijkobservatie II: overheidsorganisaties die met een grote verscheidenheid aan informatieveiligheidsregels te maken hebben, beoordelen vanuit efficiencyoverwegingen niet of informatiesystemen aan alle regels voldoen, maar controleren compliance aan informatieveiligheidsregels wanneer daar aanleiding voor is	21
4.3	Praktijkobservatie III: in ketensamenwerkingen worden informatieveiligheidseisen gesteld, maar er wordt weinig ingezet op het controleren van de naleving van deze eisen.	22
5	**Aanbevelingen**	**23**
5.1	Inleiding	23
5.2	Samenvattende bevindingen	23
5.3	Vier aanbevelingen	25

Bijlage A: De onderzochte informatieveiligheidsregels **29**

Bijlage B: De uitwerking van twee personae **46**

1 INLEIDING

1.1 Achtergrond en onderzoeksopdracht

Waar het gaat om de verbetering van informatieveiligheid bij de overheid neemt het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (**het ministerie van BZK**) de verantwoordelijkheid om overheidsbrede samenwerking te stimuleren en daar waar het kan en nodig is randvoorwaardelijke kaders op te stellen.[1] Het ministerie vult deze verantwoordelijkheid op verschillende manieren in. Voorbeelden hier van zijn de Agenda Digitale Overheid (NL DIGIbeter) en het stimuleren en ondersteunen van de implementatie van de Baseline Informatiebeveiliging Overheid (**BIO**) door overheidsorganisaties.

In dit rapport wordt de aandacht gericht op het kaderstellende aspect van de verantwoordelijkheid van het ministerie: het vertalen van minimumeisen ten aanzien van informatieveiligheid naar een regelgevend kader. Dit betekent dat BZK zelf regelgeving kan voorstellen en regie kan voeren op dit thema om de informatiebeveiliging van overheidsorganisaties te versterken.

Deze algemene kaderstellende verantwoordelijkheid voor informatieveiligheid bestaat naast sectorale verantwoordelijkheid voor informatieveiligheid. Daardoor bestaan er, naast algemene regels over informatieveiligheid, ook andere, informatieveiligheidsregels die door sectorale overheidsorganisaties zijn gesteld. Dit heeft geleid tot informatieveiligheidsregels in het sociale, fysieke en – veiligheidsdomein die op Rijks, provinciaal, gemeentelijk en waterschapniveau zijn vastgesteld. Deze regels dragen bij aan het regelgevend kader voor informatieveiligheid. Voor het ministerie van BZK is het daarom zinvol om overzicht en inzicht te krijgen in alle informatieveiligheidsregels die voor Nederlandse overheidsorganisaties gelden.

Om tot een dergelijk overzicht en inzicht te komen, heeft het ministerie van BZK aan Berenschot en VKA de opdracht gegeven om onderzoek te doen op basis van twee onderzoeksvragen:

1. Onderzoek bestaande wet- en regelgeving kaderstelling vanuit de rijksdienst en vanuit medeoverheden;

2. Onderzoek bestaande problemen bij de uitwisseling van informatie binnen en tussen overheidslagen en met aan de overheid gelieerde organisaties.

Het inzicht in de regels voor informatieveiligheid van overheidsorganisaties dient ter nadere onderbouwing voor een integraal afwegingskader (IAK) Informatieveiligheid.

Naast het geven van overzicht en inzicht bevat dit rapport ook aanbevelingen voor de manier waarop het ministerie van BZK de verantwoordelijkheid voor het regelgevend kader kan invullen.

[1] Zie ook: Kamerstukken II 2018/2019, nr. 574.

1.2 Aanpak van het onderzoek

1.2.1 Afbakening van het onderzoek

Dit onderzoek gaat over informatieveiligheidsregels bij overheidsorganisaties. Bij het onderzoek zijn de kernbegrippen van het onderzoek gedefinieerd. Productvoorschriften aan informatiesystemen vallen niet onder informatieveiligheidsregels. Ze zijn wel relevant voor de informatieveiligheid, maar worden niet meegenomen in het onderzoek.

1.2.2 Definities

Ter afbakening van het onderzoeksgebied worden in dit onderzoek de volgende definities gehanteerd:

REGELS

Op basis van de uitvraag worden regels gedefinieerd als:

> *wet- en regelgeving en kaderstelling vanuit de rijksdienst en vanuit medeoverheden*

Regels over informatieveiligheid zijn te vinden in wetten, besluiten, regelingen, beleidsregels, convenanten, interne afspraken, standaarden (bijvoorbeeld ISO/NEN) en een groot aantal andere documenten.

INFORMATIEVEILIGHEIDSREGELS EN INFORMATIEBEVEILIGING

Bij de vaststelling over wat regels over informatieveiligheid zijn, is aangesloten bij de definitie van **informatiebeveiliging** in de Baseline Informatiebeveiliging Overheid, die de definitie uit het Besluitvoorschrift informatiebeveiliging 2007 (VIR) (artikel 1, sub a) gebruikt. Deze definitie luidt:

> *Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen*

Informatieveiligheid is het effect van informatiebeveiliging. **Informatieveiligheidsregels** zijn daarmee regels over informatiebeveiliging die beogen tot informatieveiligheid te komen.

GEGEVENS

In dit rapport worden, net als in de definitie uit de VIR, de termen gegevens en informatie gebruikt als synoniemen. Voor dit onderzoek is het nuttig om voor gegevens een definitie te hanteren die aansluit bij de splitsing tussen persoonsgegevens en andere typen gegevens.

> *persoonsgegevens en andere typen gegevens* [2]

[2] Ook de Wet op inlichtingen- en veiligheidsdiensten 2017 houdt het onderscheidt tussen persoonsgegevens en andere gegevens aan (art. 1, sub d, Wiv 2017).

Voor de definitie van persoonsgegevens bij de definitie uit de Algemene verordening gegevensbescherming (**AVG**):

> *gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon*

GERICHT OP OVERHEIDSORGANISATIES

Dit onderzoek richt zich op de regels over informatieveiligheid die gelden voor de overheidsorganisaties. Voor het komen tot een zo volledig mogelijk beeld van de bestaande regelgeving is van belang te weten voor welke partijen welke eisen gelden. Met overheidsorganen wordt in dit onderzoek bedoeld bestuursorganen in de zin van de Algemene wet bestuursrecht (**Awb**). Dit omvat bestuursorganen binnen alle overheidslagen:

- Rijksoverheid
- Provincies
- Gemeenten
- Waterschappen.

In wetgevingstermen wordt over ook wel over “normadressaten” gesproken. In dit onderzoek wordt de term overheidsorganisaties en bestuursorganen aangehouden. In overleg met de opdrachtgever is niet voor ieder type bestuursorgaan een diepteanalyse gedaan op de regelgeving inzake informatieveiligheid.

1.2.3 Verantwoording methode bureau- en casusonderzoek

Dit onderzoek is opgesteld met behulp van een combinatie van bureau- en casusonderzoek, sessies met verschillende experts van VKA en Berenschot en regelmatige overleggen met de opdrachtgever. De onderzoeksgegevens die de onderzoeken, sessies en overleggen opleverden vormen gezamenlijk het onderzoek naar bestaande wet- en regelgeving kaderstelling vanuit de rijksdienst en vanuit medeoverheden en de bestaande problemen bij de uitwisseling van informatie binnen en tussen overheidslagen en met aan de overheid gelieerde organisaties.

KEUZES BIJ DE UITVOERING VAN BUREAU- EN CASUSONDERZOEK

De inventarisatie van de bestaande regelgeving is gebruik gemaakt van on- en offlinebronnen. Ook is gebruik gemaakt van een aantal experts van VKA en Berenschot op het gebied van informatieveiligheid om de inventarisatie verder aan te vullen.

Bij de te onderzoeken casussen is gekozen om een belangrijk element uit de definitie van informatieveiligheid te combineren met een multisectoraal onderzoek. In de definitie van informatieveiligheid speelt het onderscheid **vertrouwelijkheid, beschikbaarheid en integriteit** een belangrijke rol. De regels over informatieveiligheid zijn in verschillende sectoren gesteld. Om een

voldoende beeld te krijgen, is gekozen om de casussen zo te organiseren dat het sociale-, fysieke- en veiligheidsdomein naar voren komen en gecombineerd worden met de drie onderscheidingen uit de definitie van informatieveiligheid. Daarbij is gekozen om in elke sector te focussen op een van de drie aspecten uit informatieveiligheid.

1.2.4 Leeswijzer

Hoofdstuk 2 geeft een overzicht van de typologieën van regels die in dit onderzoek zijn aangetroffen. Hier wordt inzicht gegeven in de verschillen die er zijn op de inhoud van informatieveiligheidsregels en de manieren waarop deze gesteld worden. Het overzicht van de onderzochte informatieveiligheidsregels is opgenomen in **Bijlage A.**

Hoofdstuk 3 gaat dieper in op een aantal belangrijke thema's binnen informatieveiligheidsregels en de dagelijkse praktijk. Informatieveiligheidsregels in ketensamenwerkingen, de uitwerking van toezicht, handhaving, verantwoording en governance en tot slot de relatie tussen producteisen en informatieveiligheidsregels.

Hoofdstuk 4 bevat een weergave van de observaties die in dit onderzoek zijn gedaan door interviews te houden met mensen die in de praktijk te maken hebben met de verschillende informatieveiligheidsregels. In Bijlage B zijn de verschillende interviews samengevoegd in de omschrijving van twee personae en geven het effect weer die deze regels hebben op de dagelijkse praktijk.

In Hoofdstuk 5 bevat de samenvattende bevindingen op basis de voorgaande hoofdstukken en vier aanbevelingen ten aanzien van het stellen van informatieveiligheidsregels voor overheidsorganen in het algemeen en het effect dat deze hebben in de praktijk.

2 TYPOLOGIËN VAN INFORMATIEVEILIGHEIDSREGELS

2.1 Inleiding

Er is op het gebied van informatieveiligheid een veelheid aan regels, opgesteld door veel verschillende organisaties en op verschillende manieren. In **Bijlage A** is een overzicht opgenomen van de 98 wettelijke en 14 niet wettelijke documenten die in het kader van dit onderzoek zijn onderzocht. Deze documenten zijn de informatieveiligheidsregels in wetgeving, regelgeving en kaderstelling vanuit de rijksdienst en vanuit medeoverheden. Van enkele belangrijke documenten met informatieveiligheidsregels is daarbij in Bijlage A een toelichting opgenomen.

In dit hoofdstuk worden de informatieveiligheidsregels uit Bijlage A getypeerd. Dit leidt tot een typologie van informatieveiligheidsregels aan de hand van:

1. de inhoud van de regels (paragraaf 2.2);
2. de manier waarop de regels zijn gesteld (paragraaf 2.3).

2.2 Drie categorieën van informatieveiligheidsregels

Om op een overzichtelijke manier informatieveiligheidsregels weer te kunnen geven, zijn op basis van een analyse van de informatieveiligheidsregels in de bijlage, algemene wetgevingsleer en een aantal expertsessies, drie categorieën van informatieveiligheidsregels geïdentificeerd. Dit leidt tot een indeling van alle informatieveiligheidsregels in drie uitsluitende categorieën. Alle regels die zijn onderzocht kunnen worden ondergebracht in één of meerdere van de volgende categorieën:

1. Regels betreffende de **inhoudelijke** eisen aan informatieveiligheid. Dit zijn regels die zien op:
   a. vertrouwelijkheid, waaronder:
      1. authenticatie;
      2. identificatie;
      3. gegevensdeling;
      4. autorisatie;
   b. beschikbaarheid;
   c. integriteit.

2. Regels betreffende de **toepassing** van de inhoudelijke eisen (wanneer zijn de regels op wie van toepassing?). Dit zijn regels die zien op:
   a. wie de regel van toepassing is;
   b. de omstandigheden waaronder de regel van toepassing is (rechtsfeit);
   c. de plaats waar de regel van toepassing is;
   d. de tijd waarop de regel van toepassing is.

3. Regels betreffende **toezicht, handhaving, verantwoording en governance** (eventueel ook: certificering). Dit zijn regels die zien op:
   a. functionele verantwoording;
   b. democratische verantwoording;

c. toezicht en handhaving (waaronder sanctionering);
d. certificering;
e. governance;
f. algemene bestuurlijk zorgplicht.

De in de bijlage opgesomde documenten bevatten regels die in één of meerdere van deze categorieën vallen.

Een goed voorbeeld van de laatste situatie biedt artikel 7.2.2 van het Besluit Jeugdwet. Deze bepaling luidt als volgt:

1. *Een instantie die behoort tot een van de categorieën, bedoeld in de artikelen 7.1.1 tot en met 7.1.7 of een functionaris die behoort tot een van de categorieën, bedoeld in artikel 7.1.3, tweede lid, of 7.1.4, tweede lid, draagt zorg voor een zorgvuldig en veilig gebruik van de verwijsindex.*
2. *Een instantie of een functionaris wordt vermoed te voldoen aan het bepaalde in het eerste lid als deze voldoet aan de eisen zoals deze zijn uitgegeven door het Nederlands Normalisatie-instituut in de NEN 7510, Medische informatica – Informatiebeveiliging in de zorg – Algemeen.*

Artikel 7.2.2. van het Besluit Jeugdwet bevat informatieveiligheidsregels die in de drie categorieën vallen.

- Het eerste lid bevat regels over de **toepassing**. Er wordt bepaald op wie de regel van toepassing is (een instantie of functionaris) en de omstandigheden waaronder de regel van toepassing is (het gebruik van een verwijsindex).
- Het tweede lid bevat een (overigens zeer open geformuleerde) **inhoudelijke** eis aan het "zorgvuldig en veilig gebruik van de verwijsindex". De wetgever geeft deze open norm nader in te vullen door aan te geven dat een instantie of functionaris wordt "vermoed te voldoen" aan de inhoudelijke eisen wanneer het voldoet aan NEN7510, die meer invulling geeft aan de inhoudelijke eisen.
- Het tweede lid bevat ook regels over **verantwoording** door te verwijzen naar NEN7510. In deze standaard staan namelijk niet alleen inhoudelijke eisen, maar ook eisen aan de governance op en verantwoording over de inhoudelijke eisen.

2.3 Vijf manieren om informatieveiligheidsregels te stellen

2.3.1 Introductie

De drie categorieën van informatieveiligheidsregels worden niet op een eenduidige manier gesteld. Wetgevers, regelgevers en kaderstellers hebben een aantal keuzes bij het opstellen van informatieveiligheidsregels. Deze keuzes zijn weer te geven op twee spectrums.

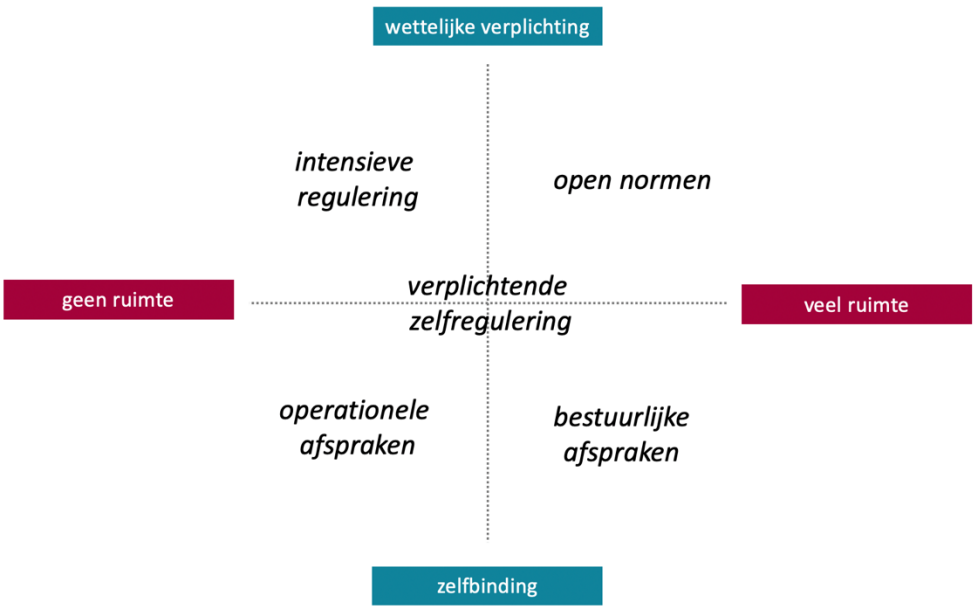
Het eerste spectrum loopt van wettelijke verplichting naar zelfbinding.

- Het ene uiterste van het spectrum vormen de informatieveiligheidsregels in de vorm van wettelijke verplichtingen. Deze verplichtingen hebben meestal de vorm van wetten in formele zin, algemene maatregelen van bestuur, ministeriële regelingen en provinciale, gemeentelijke of waterschapsverordeningen.
- Het andere uiterste zijn informatieveiligheidsregels waaraan een overheid zichzelf uit vrije wil committeert. Dit is zelfbinding in de vorm van convenanten, akkoorden en interne regels.

Het tweede spectrum aan keuzes voor opstellers van informatieveiligheidsregels ziet op de mate waarin overheidsorganisaties de ruimte hebben om zelf invulling te geven aan de informatiebeveiliging.

- Het ene uiterste van het spectrum ziet op informatieveiligheidsregels die een zodanige uitputtende regeling bevatten dat overheidsorganisaties geen ruimte hebben om eigen keuzes te maken.
- Het andere uiterste is de situatie dat informatieveiligheidsregels aan overheidsorganisaties veel ruimte laten om zelf keuzes te maken over de inrichting van de informatiebeveiliging.

Door deze twee spectrums te combineren, ontstaat het volgende kwadrant (figuur 1):



Figuur 1: Verhouding van keuzes ten aanzien van het opstellen van informatieveiligheidsregels

Binnen dit kwadrant zijn vijf manieren om informatieveiligheidsregels op te stellen ingetekend:

1. **Intensieve regulering**: dit zijn wettelijke verplichtingen voor overheidsorganisaties die weinig ruimte laten voor eigen invulling van de informatiebeveiliging.

2. **Open normen**: dit zijn wettelijke verplichtingen die veel ruimte laten voor een eigen uitwerking.
3. **Bestuurlijke afspraken**: dit zijn afspraken over informatiebeveiliging waaraan een overheidsorganisatie zich bindt en die veel ruimte laten voor eigen uitwerking.
4. **Operationele afspraken**: dit zijn afspraken over informatiebeveiliging waaraan een overheidsorganisatie zich bindt en die weinig ruimte laten voor eigen uitwerking.
5. **Verplichtende zelfregulering**: dit zijn niet-vrijblijvende, bindende afspraken op tactisch niveau, waaraan overheidsorganisaties zichzelf committeren.

Het vervolg van dit hoofdstuk bevat voorbeelden van deze vijf manieren om informatieveiligheidsregels op te stellen en verklaringen waarom opstellers van regelgeving hiervoor kiezen. Ook in het vervolg van dit onderzoek wordt dit kwadrant gebruikt voor de analyse.

2.3.2 Voorbeelden van en verklaringen voor intensieve regulering

Er is sprake van intensieve regulering wanneer de drie categorieën van informatieveiligheidsregels voor een groot deel in wetgeving zijn vastgelegd. Een voorbeeld uit het veiligheidsdomein biedt de Regeling informatiebeveiliging politie. Deze regeling beoogt een samenhangend pakket van maatregelen te treffen en te onderhouden “ter waarborging van de beschikbaarheid, integriteit en exclusiviteit[3] van een informatiesysteem en de informatie daarin. De intensieve regulering is bijvoorbeeld goed zichtbaar in artikel 4 van de regeling in combinatie met bijlage I (betrouwbaarheidscriteria en normklassen). Daarin staat een zorgplicht voor de korpschef met een sectorspecifieke en verplichte uitwerking van deze zorgplicht (“deze zorgplicht houdt tenminste in dat:”). Hoewel deze regeling niet alle mogelijk ruimte voor de korpschef invult, is het een voorbeeld van intensieve regulering. In dit geval heeft de wetgever gekozen voor een uitwerking van alle beveiligingsmaatregelen en niet voor open normen. De wetgever heeft hier weinig ruimte voor eigen uitwerking overgelaten.

Een ander voorbeeld van intensieve regulering zijn de aansluitvoorwaarden die gelden voor het gebruik van de Collectieve Opdracht Routeer Voorziening (CORV). Dit is een voorziening van Justid die gemeenten en justitiële partijen gebruiken om informatie over jeugdigen uit te wisselen. Voor het aansluiten aan de CORV zijn aansluitvoorwaarden opgesteld in de Regeling justitiële keteninformatisering Jeugdwet. Van deze aansluitvoorwaarden mag niet afgeweken worden.

De keuze om in een aantal situaties intensiever te reguleren is verklaarbaar op basis van de aard van de gegevens. Essentiële informatie en (bijzondere) persoonsgegevens hebben speciale aandacht van de wetgever.

Een goed voorbeeld van aandacht voor essentiële informatie is zichtbaar in de Wet Beveiliging Netwerk- en Informatiesystemen (**Wbni**). Deze wet is een omzetting van de NIB-richtlijn. In deze

[33] Exclusiviteit wordt hier gebruikt als een andere term voor vertrouwelijkheid.

wet worden “aanbieders van essentiële diensten” en “digitale dienstverleners” aangewezen waarop de Wbni-wetfamilie van toepassing is. Een aanbieder is essentieel wanneer het een dienst verleent die van “essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten, de verlening van de dienst afhankelijk is van netwerk- en informatiesystemen en een incident aanzienlijke verstorende effecten zou hebben voor de verlening van de dienst” (artikel 5, tweede lid, NIB-richtlijn). Anders gezegd, omdat het te beveiligen proces en de daarin vervatte informatie een groot maatschappelijk belang heeft, kiest de wetgever ervoor om de informatiebeveiliging strenger te reguleren en minder ruimte te laten.

Een vergelijkbare rationale is zichtbaar in de Wet justitiële en strafvorderlijke gegevens (**Wjsg**). Deze wet ziet op strafrechtelijke persoonsgegevens, die vanwege hun aard zeer gevoelig zijn. Belangrijk daarbij is dat de Wjsg niet alleen inhoudelijke informatiebeveiligingseisen regelt, maar ook de burger waarborgen biedt tegen ongerechtvaardigde inbreuken op de persoonlijke levenssfeer.

Dit past in een breder principe rondom informatiebeveiliging; de informatiebeveiliging van (bijzondere) persoonsgegevens heeft meer aandacht van wetgevers, regelgevers en kaderstellers dan de informatiebeveiliging van niet-persoonsgegevens. Dit principe kent meerdere aspecten. De potentiele omvang en impact van de schade bij persoonsgegevens is groot. Bij persoonsgegevens ontstaat de schade primair bij de individu die een sterke afhankelijkheidsrelatie heeft met de overheid. Dit principe zie je ook terug de beginselen van in de AVG, die bij de bescherming van persoonsgegevens de betrokkene op wie de persoonsgegevens betrekking heeft, centraal stelt. Door regelgeving als de AVG en het toezicht op de naleving daarvan is de aandacht voor de bescherming van persoonsgegevens groter geworden.

2.3.3 Voorbeelden van en verklaringen voor open normen

Er is sprake van open normen wanneer een wetgever weliswaar informatiebeveiligingsregels heeft gesteld, maar deze niet uitwerkt of zich alleen beperkt tot één of twee categorieën van informatieveiligheidsregels. Een voorbeeld van deze manier van regelstellen is artikel 7.2.2 van het Besluit Jeugdwet. Deze bepaling luidt als volgt:

1. *Een instantie die behoort tot een van de categorieën, bedoeld in de artikelen 7.1.1 tot en met 7.1.7 of een functionaris die behoort tot een van de categorieën, bedoeld in artikel 7.1.3, tweede lid, of 7.1.4, tweede lid, draagt zorg voor een zorgvuldig en veilig gebruik van de verwijsindex.*
2. *Een instantie of een functionaris wordt vermoed te voldoen aan het bepaalde in het eerste lid als deze voldoet aan de eisen zoals deze zijn uitgegeven door het Nederlands Normalisatie-instituut in de NEN 7510, Medische informatica – Informatiebeveiliging in de zorg – Algemeen.*

Deze bepaling uit de Jeugdwet is zeer bondig geformuleerd. De kern wordt gevormd door de zorgplicht in het eerste lid: “draagt zorg voor een zorgvuldig en veilig gebruik van de verwijsindex”.

Vervolgens wordt, in lijn met aanwijzing 3.48 en 3.49 van de Aanwijzingen voor de Regelgeving, verwezen naar een normalisatienorm van het Normalisatie-instituut NEN als invulling daarvan.

Zoals eerder werd besproken, zijn in deze bepaling de drie categorieën informatiebeveiligingsregels zichtbaar. Daarbij viel op dat verwezen wordt naar NEN-normen. Deze keuzes wordt vaak gemaakt vanwege de korte levenscyclus van informatietechnologieën inhoudelijke regels snel verouderd raken (bijvoorbeeld in de VIR 2007, zie Bijlage A). Van ISO en NEN verwachten bestuursorganen en regelgevers dat de regels die ze als norm stellen up-to-date zijn[4].

Verder valt op dat in deze bepaling expliciet een toepassingsbepaling staat. Deze toepassingsbepaling zorgt ervoor dat de regels worden opgelegd aan bepaalde actoren (een instantie of functionaris). Deze bepaling staat in de wetgeving om normen afdwingbaar te maken. Alleen via een democratisch gelegitimeerde wet kan een ander gedwongen worden om zich aan regels te houden middels handhaving.

2.3.4 Voorbeelden van en verklaringen voor bestuurlijke afspraken

Een voorbeeld van bestuurlijke afspraken zijn de bestuursakkoorden in de watersector. In de Waterwet wordt door de wetgever aan de minister van Infrastructuur en Water de opdracht gegeven er zorg voor te dragen dat “informatie beschikbaar is” (artikel 3.3, eerste lid, onderdeel a). Een wettelijke zorgplicht leidt doorgaans tot meer concrete bindende afspraken. Uit de memorie van toelichting blijkt dat de wetgever bij dit “zorgdragen” in eerste instantie denkt aan het sluiten van bestuursakkoorden. Dit heeft geresulteerd in een aantal bestuursakkoorden, waarvan de laatste dateert van 2018 (zie ook casus 1 in hoofdstuk 3). Als het sluiten van akkoorden onverhoopt niet lukte, had de minister gebruik kunnen maken van de grondslag in artikel 3.10 om dwingende regels te stellen. Hiervoor is echter tot op heden geen aanleiding geweest. In de watersector bestaat kennelijk geen aanleiding om afdwingbare regels te stellen en zijn bestuurlijke afspraken voldoende.

2.3.5 Voorbeelden van en verklaringen voor operationele afspraken

Voorbeelden van operationele afspraken zijn moeilijker in regelgeving te vinden omdat dit soort afspraken vaak tussen overheden worden gemaakt en niet altijd openbaar gemaakt worden als regelgeving of bestuurlijke afspraken. Een voorbeeld van operationele afspraken over informatieveiligheid is het convenant van 25 juni 2014 tussen het waterschap Zuiderzeeland, Rijkswaterstaat Midden-Nederland en de veiligheidsregio Flevoland. In artikel 15 van dit convenant staat dat partijen er naar streven te werken volgens de netcentrische wijze van informatievoorziening en daarbij gebruik gaan maken van de netcentrische applicatie van de

[4] Dit betekent overigens niet dat ISO- en NEN-standaarden heel vaak veranderen. De kracht is ook de toekomstvaste formulering van deze standaarden en de omvangrijk beheercyclus ervan. Dit betekent wel dat de standaarden vooral aandachtsgebieden en algemene normen bevatten die organisaties zelf in concrete uitwerkingen moeten worden geoperationaliseerd.

veiligheidsregio. Deze applicatie is het Landelijk Crisismanagement Systeem (LCMS). Het waterschap en Rijkswaterstaat zijn niet verplicht om gebruik te maken van het LCMS, maar sluiten hiermee aan op het systeem dat de veiligheidsregio gebruikt om zo de informatie-uitwisseling zo eenvoudig mogelijk te maken.

2.3.6 Voorbeeld van en verklaring voor verplichtende zelfregulering

Recent is voor alle overheidslagen de Baseline Informatiebeveiliging Overheid (BIO) in werking getreden. De BIO Is een voorbeeld van niet-vrijblijvende, bindende afspraken op tactisch niveau, waaraan overheidsorganisaties zichzelf hebben gecommitteerd. De informatieveiligheidsregels in de BIO zijn in de vorm van maatregelen en controls gesteld. Deze tactisch vormgegeven baseline kan in theorie weer verder uitgewerkt worden op operationeel niveau en in de praktijk moet dit door het eigen opgelegde risicomanagement. Het zijn deze operationele uitwerkingen waarmee de mensen die dagelijks actief zijn voor de informatieveiligheid bij overheidsorganisaties werken. Op deze manier ontstaan er op verschillende niveaus informatieveiligheidsregels die met elkaar samenhangen.

2.4 Conclusie typering informatieveiligheidsregels en regelgevingspatronen

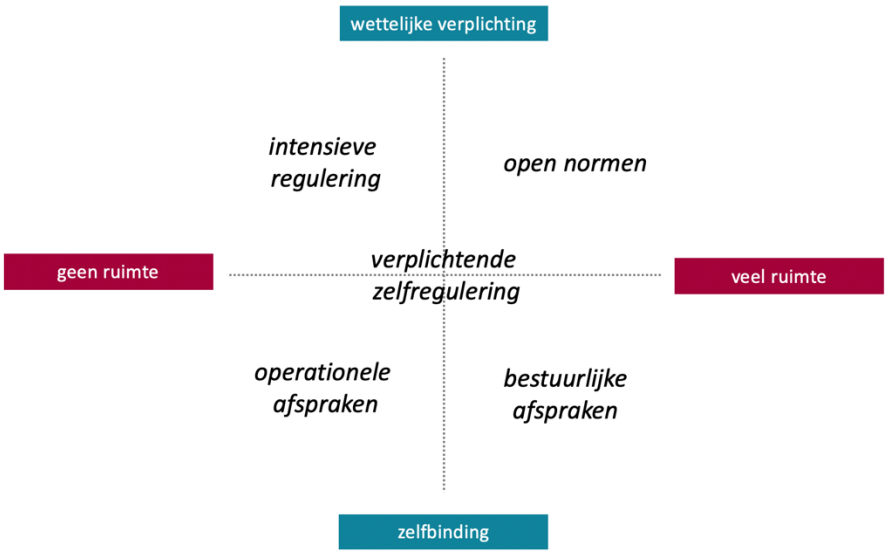
In dit hoofdstuk 2 is na een analyse van de documenten in Bijlage A een typologie van informatieveiligheidsregels geschetst aan de hand van:

1. de onderwerpen van de regels (regels over inhoud, verantwoording en toepassingsbereik, paragraaf 2.2);
2. vijf manieren waarop de regels zijn gesteld (intensieve regulering, open normen, bestuurlijke akkoorden, operationele afspraken en verplichtende zelfregulering, paragraaf 2.3).

Deze typologieën maken het mogelijk om informatieveiligheidsregels consequent te analyseren. Dit maakt het mogelijk om patronen waar te nemen in de manier waarop welk type regels vaak worden gesteld. Op basis van de paragrafen 2.2 en 2.3 zijn ten minste vier **regelgevingspatronen** te identificeren.

2.4.1 Regelgevingspatroon 1: er is veel diversiteit in de manier waarop informatieveiligheidsregels worden gesteld

De huidige inrichting van informatieveiligheidsregels biedt de verschillende overheidsorganisaties in het sociale, fysieke en veiligheidsdomein veel ruimte om zelf de manier van regels stellen te bepalen. Daardoor worden op informatieveiligheidsregels op veel verschillende manieren gesteld. Deze manieren zijn weer te geven in het eerder al opgevoerde kwadrant:



2.4.2 Regelgevingspatroon 2: open normen en standaarden worden vaak gecombineerd

Opstellers van informatieveiligheidsregels combineren vaak open normen met verwijzingen naar ISO en NEN-normen.

2.4.3 Regelgevingspatroon 3: bij bepalen van het toepassingsbereik van regels staan de aard van de gegevens (meestal) centraal

De regels over toepassingsbereik van informatieveiligheidsregels zien de vraag: wanneer zijn de regels op wie van toepassing? Bij het antwoord op deze vraag is het soort gegevens vrijwel altijd bepalend. Bijvoorbeeld, wanneer er sprake is van een bijzonder persoonsgegeven leidt dat meteen tot de toepassing van een set aan informatieveiligheidsregels. Anders gezegd: juridisch gezien is de aard van de gegevens vaak de trigger voor het aan-of-uit-gaan van een regelgevend kader.
Dit maakt de vraag welke gegevens beveiligd moeten worden, de absolute kernvraag. Dit is vaak geen eenvoudig te beantwoorden vraag. Het kan zijn dat één gegeven, tegelijkertijd meerdere statussen heeft en daarmee meerdere regelgevende kaders van toepassing maakt. Ook kan een gegevensbestand meerdere typen gegevens bevatten.

2.4.4 Regelgevingspatroon 4: de mate van noodzaak tot afdwingbaarheid verklaart vaak de wijze van regelgeven

In een sector waarin een duidelijk gedeeld belang is en alle partijen tot de overheid behoren (zoals de watersector), is meer sprake van zelfbinding dan in sectoren waarin private en publieke partijen met verschillende belangen samenwerken. Anders gezegd, opstellers kiezen voor bestuurlijke en operationele afspraken wanneer er geen noodzaak tot afdwingbaarheid gevoeld wordt.

3 BELANGRIJKE THEMA'S VOOR INFORMATIEVEILIGHEIDSREGELS

3.1 Introductie

Het vorige hoofdstuk bevatte een typering van de informatieveiligheidsregels voor overheidsorganisaties. Deze typering maakt het mogelijk om informatieveiligheidsregels te analyseren en regelgevende patronen te identificeren. Tijdens de analyse kwamen drie belangrijke thema's voor informatieveiligheidsregels naar voren, waarop in dit hoofdstuk ingezoomd wordt. Het betreft:

1. Informatieveiligheidsregels in ketensamenwerkingen (3.2);
2. Regels over toezicht, handhaving, verantwoording en governance (3.3);
3. Wettelijke producteisen en informatieveiligheidsregels (3.4).

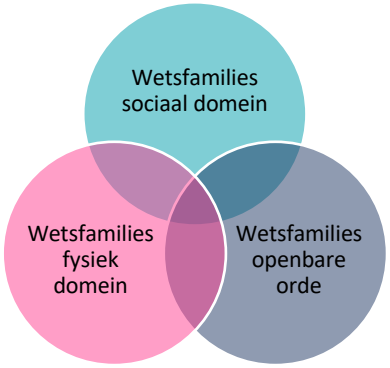
3.2 Informatieveiligheidsregels in ketensamenwerkingen

Veel overheidsorganisaties wisselen informatie uit in ketens. Binnen deze ketens is de uitwisseling van informatie vaak gereguleerd door overeenkomsten, convenanten, protocollen en vergelijkbare al dan niet bindende privaatrechtelijke instrumenten. Overheidsorganisaties kiezen er regelmatig voor om in dergelijke instrumenten informatieveiligheidseisen te stellen. Deze informatieveiligheidseisen zijn vaak een doorvertaling van de eisen die voor deze overheidsorganisaties zelf gelden.

Er zijn op hoofdlijnen drie typen ketens en binnen deze type ketens ontstaan in meer of mindere mate problemen met informatieveiligheidsregels.

1. Ketens binnen een bestuursorgaan (interne ketens)
In deze ketens ontstaan doorgaans geen problemen met informatieveiligheidsregels bij de uitwisseling van informatie. In deze gevallen kan een bestuursorgaan zelf de informatieveiligheidsregels in de gehele keten bepalen en aanpassen, mochten deze de informatie-uitwisseling onnodig beperken.

2. Ketens met bestuursorganen (publiek-publieke ketens)
In deze ketens ontstaan, in potentie, problemen met informatieveiligheidsregels doordat verschillende wetsfamilies op de informatie-uitwisseling in de keten van toepassing zijn. Vooral besturen die in meerdere domeinen actief zijn, hebben hier mee te maken. Het schoolvoorbeeld zijn gemeenten waarvoor binnen de wetsfamilies in de verschillende domeinen informatieveiligheidsregels bestaan. Dit kan ertoe leiden dat hetzelfde stukje informatie aan verschillende wetsfamilies moet voldoen. Deze regels zijn vaak niet op elkaar afgestemd.



Figuur 2: Overlap in sectorale wetsfamilies

3. **Ketens met bestuursorga(a)n(en) en private organisatie(s) (publiek-private ketens).**
In deze ketens wisselen private en publieke organisaties informatie met elkaar uit. De problemen die samenhangen met de publiek-publieke ketens spelen ook in deze situaties. Specifiek voor deze ketens speelt de vraag op welke manier de publieke partijen toezicht houden op de manier waarop private partijen de informatieveiligheidsregels toepassen (zie ook volgende paragraaf).

3.3 Regels over toezicht, handhaving, verantwoording en governance

Speciale aandacht verdient de categorie regels over toezicht, handhaving, verantwoording en governance (eventueel ook: certificering). Dit zijn regels die zien op:

- functionele verantwoording;
- democratische verantwoording;
- toezicht en handhaving (waaronder sanctionering);
- certificering;
- governance;
- algemene bestuurlijk zorgplicht.

Deze brede categorie regels wordt op zeer uiteenlopende manieren gesteld. In sommige gevallen staan er hoge sancties op het schenden van informatieveiligheidsregels. Een goed voorbeeld is de Wet bescherming staatsgeheimen, in combinatie met het Wetboek van Strafrecht. Het schenden van informatieveiligheidseisen in de Wet bescherming staatsgeheimen kan leiden tot een gevangenisstraf van ten hoogste zes jaren.[5] Anderzijds bevatten deze categorie regels ook niet-afdwingbare, bestuurlijke akkoorden over de samenwerking tussen overheidsorganisaties.

Eenzelfde verschil is waarneembaar tussen regels over functionele verantwoording en democratische verantwoording. De regels over functionele verantwoording (ook wel verticale verantwoording) hebben de vorm van wettelijk verplichtingen (Wet Suwi, Digid). Op deze regels wordt op een fijnmazige manier toezicht gehouden en zijn voldoende handhavingsinstrumenten voorhanden. De regels over democratische verantwoording komen voort uit algemene regels over de staatkundige verhouding tussen volksvertegenwoordiging en bestuur. Bij democratische verantwoording past een heel ander soort toezicht en handhaving. Toezicht is afhankelijk van de belangstelling van de volksvertegenwoordiging en handhaving (om het zo te noemen), loopt via het vertrouwensbeginsel.

Een ander relevant verschil voor deze categorie regels is de aard van de gegevens. Voor persoonsgegevens is altijd toezicht, handhaving en sanctionering beschikbaar via het vangnet van de AVG (en onderliggende regelgeving). Burgers kunnen zelf handhaving van de bepalingen uit de AVG vorderen en er is een duidelijke toezichthouder, met stevige toezicht- en handhavingsinstrumenten (de autoriteit persoonsgegevens), die overheden kan sanctioneren.

[5] Artikel 98, tweede lid, Wetboek van Strafrecht.

Niet-persoonsgegevens hebben niet een dergelijk vangnet, behalve in het strafrecht. Of deze regels gehandhaafd worden, is daarmee afhankelijk van sectorale regelgeving.

3.4 De relatie tussen wettelijke producteisen en informatieveiligheidsregels

Veel overheidsorganisaties gebruiken apparaten en software die informatie verzamelen en doorgeven. In het oog springen computers en telefoons, maar met bijvoorbeeld de opkomst van het *internet of things* (IoT) neemt het aantal apparaten dat informatie verzamelt en doorgeeft toe. Te denken valt aan koelkasten in overheidsgebouwen of verkeerslichten op straat. Deze apparaten verzamelen steeds meer informatie en geven informatie door en zijn daarmee potentieel een risico voor de informatieveiligheid.

Op de vereiste beveiliging van dit *proces* van informatieverzameling- en uitwisseling door apparaten zien informatieveiligheidsregels. Sterk gelieerd aan de informatieveiligheidsregels zijn de (technische) *eisen aan apparaten en de software*. Deze wettelijke producteisen zien niet op de beveiliging van het proces van informatieverzameling en -deling, maar op het apparaat of de software waarmee de informatie verzameld en gedeeld wordt. De verantwoordelijkheid voor de producteisen is anders belegd dan die voor informatieveiligheidsregels: deze wettelijke producteisen worden doorgaans op Europees niveau gesteld. De Europese wetgever geeft het stellen van afdwingbare, wettelijke producteisen veel prioriteit omdat ze noodzakelijk zijn voor het inrichten van een Europese interne markt. Het belang van goede producteisen blijkt ook uit twee publicaties van de Cyber Security Raad (CSR) uit 2017: '*Naar een veilig verbonden digitale samenleving*' [6] en '*Ieder bedrijf heeft digitale zorgplichten*' [7].

De wettelijke producteisen bevatten meestal gedetailleerde technische eisen, die ook kunnen zien op het beveiligen van de informatieverzameling en -uitwisseling door een apparaat. Als hiervan sprake zou zijn, komen er binnen de Europese Unie alleen producten op de markt die veilig informatie verzamelen en uitwisselen.

Een product dat vanwege wettelijke producteisen die zien op de informatieverzameling en -uitwisseling veilig informatie verzamelt en uitwisselt, vraagt om minder regels rondom informatieveiligheid. Daardoor is er in een dergelijke situatie ook minder noodzaak om voor deze apparaten of software specifieke informatieveiligheidsregels op te stellen die de informatieveiligheid te garanderen. Omgekeerd, als er geen wettelijke producteisen zijn die zien op veilige informatieverzameling en -uitwisseling, is de wettelijke waarborging van informatiebeveiliging minder gegarandeerd. In dat geval moeten de regels van informatieveiligheid daarop gericht worden.

[6] Zie: https://www.cybersecurityraad.nl/binaries/CSR_Advies_IoT_NED_DEF_tcm107-314537.pdf

[7] Zie: https://www.cybersecurityraad.nl/binaries/Handreiking_Zorgplichten_NED_DEF_tcm107-314470.pdf

3.5 Conclusie 3 drie belangrijke thema's voor informatieveiligheidsregels

Op basis van de analyse van de documenten in bijlage A aan de hand van de typologieën in hoofdstuk 2 kwamen drie belangrijke thema's voor informatieveiligheidsregels naar voren:

1. Informatieveiligheidsregels in ketensamenwerkingen (3.2)
2. Regels over toezicht, handhaving, verantwoording en governance (eventueel ook: certificering) (3.3)
3. Wettelijke producteisen en informatieveiligheidsregels (3.4).

Op basis van de thematische uiteenzetting in dit hoofdstuk zijn, net als in hoofdstuk 2, drie **regelgevingspatronen** te identificeren.

3.5.1 Regelgevingspatroon 5: de manier waarop informatieveiligheidsregels doorwerken in ketens hangt van het type keten af

De relatie tussen informatieveiligheidsregels en de ketensamenwerkingen hangt af van de aard van de keten. Vooral ketens tussen verschillende bestuursorganen en publiek-private ketens lopen een verhoogd risico op juridische knelpunten, zoals ook gebleken is uit de interview (zie hiervoor hoofdstuk 4).

3.5.2 Regelgevingspatroon 6: de regels over toezicht, handhaving en sanctionering lopen sterk uiteen

Er zijn grote verschillen in de regels over toezicht, handhaving en sanctionering van informatieveiligheidsregels. Opstellers van regelgeving kiezen voor wettelijke verplichtingen wanneer er een noodzaak is om informatieveiligheidseisen af te dwingen. Meestal hangt deze noodzaak samen met de aard van de te beveiligen informatie. Vooral bijzondere persoonsgegevens en essentiële informatie krijgt in dat kader de aandacht. De inwerkingtreding van de AVG en vooral de afdwingbaarheid van de AVG heeft geleid tot relatief veel aandacht voor de bescherming van persoonsgegevens. De bescherming van niet-persoonsgegevens heeft minder aandacht van opstellers van informatieveiligheidsregels.

3.5.3 Regelgevingspatroon 7: regels over producteisen zijn medebepalend voor de vraag of nadere informatieveiligheidsregels nodig zijn

Er is een inverse relatie tussen wettelijke producteisen en informatieveiligheidsregels. Naarmate de wettelijke producteisen een hogere garantie bieden op de informatieveiligheid van een product, is er minder noodzaak voor informatieveiligheidsregels.

4 PRAKTIJKOBSERVATIES OVER DE DOORWERKING VAN INFORMATIEVEILIGHEIDSREGELS IN DE PRAKTIJK

Op basis van de onderzoeksgegevens die zijn gegenereerd uit het bureauonderzoek, de interviews, de expertsessies en de overleggen met de opdrachtgever zijn ook een aantal praktijkobservaties[8] te doen over de doorwerking van informatieveiligheidsregels in de praktijk. Deze praktijkobservaties worden geïllustreerd aan de hand van twee personae die in Bijlage B uitgewerkt zijn. In dit hoofdstuk worden drie praktijkobservaties opgesomd.

4.1 Praktijkobservatie I: hoe informatieveiligheidsregels ook zijn opgesteld, ze worden altijd vertaald naar processen en producten die de personen op de werkvloer helpen om compliant te zijn.

De casussen in dit hoofdstuk maken duidelijk dat op de werkvloer wettelijke informatieveiligheidsregels *zelf* niet het uitgangspunt vormen voor gedrag. Zorgprofessionals of mensen die informatie-uitwisseling technisch mogelijk maken, hebben vooral te maken in vertalingen van informatieveiligheidsregels naar hun eigen context. Deze dynamiek is vooral zichtbaar bij open normen.

De juridische puzzel die gelegd moet worden om compliant te zijn aan alle regels en tegelijkertijd effectief te kunnen opereren wordt gelegd door de CISO en andere informatieveiligheidsprofessionals. Dit resulteert in trainingsprogramma's, procesbeschrijvingen en software die de mensen in de operatie helpen om compliant te zijn. Een goed voorbeeld is de aankoop van een e-mailprogramma die bijdraagt om te voldoen aan NTA 7516.

4.2 Praktijkobservatie II: overheidsorganisaties die met een grote verscheidenheid aan informatieveiligheidsregels te maken hebben, beoordelen vanuit efficiencyoverwegingen niet of informatiesystemen aan alle regels voldoen, maar controleren compliance aan informatieveiligheidsregels wanneer daar aanleiding voor is

Sommige overheidsorganisaties, vooral gemeenten, kennen meer dan 50 wettelijke bronnen van informatieveiligheidseisen. Het is ondoenlijk om al die regelgeving bij te houden en constant te controleren of informatiebeveiliging – in lijn met de regelgeving – op orde is. Onder dergelijke omstandigheden kiezen overheidsorganisaties ervoor om alleen te controleren op informatieveiligheidsregels wanneer daar een directe aanleiding voor is. Voorbeelden zijn het mogelijk maken van nieuwe initiatieven, wanneer de overheidsorganisatie nieuwe taken moet

[8] Op basis van deze onderzoeksgegevens is het niet mogelijk om algemene uitspraken te doen over de impact van de manier waarop informatieveiligheidsregels zijn gesteld op de dagelijkse praktijk van professionals. Wel is het mogelijk om een drietal praktijkobservaties te doen over de doorwerking van informatieveiligheidsregels in de praktijk

uitvoeren, of wanneer er nieuwe informatie-uitwisseling tussen ketenpartijen moet worden ingericht.

4.3 Praktijkobservatie III: in ketensamenwerkingen worden informatieveiligheidseisen gesteld, maar er wordt weinig ingezet op het controleren van de naleving van deze eisen.

In veel ketensamenwerkingen participeren partijen op basis van gelijkwaardigheid. Voor het uitwisselen van informatie worden wel eisen gesteld, vaak in convenanten. In theorie wisselen overheidsorganisaties alleen informatie uit wanneer de beveiliging van deze informatie bij de andere overheidsorganisaties gegarandeerd is. Dit blijkt echter in de praktijk vooral een papieren werkelijkheid. De personen die informatie uitwisselen zijn niet actief bezig te controleren of de informatiebeveiliging bij de andere partij op orde is. Soms wordt de papieren werkelijkheid getest door bijvoorbeeld pentesten of vormen van externe controle. Verder is het belang om informatie uit te wisselen groter dan het belang van een overheidsorganisatie om de informatiebeveiliging van een andere overheidsorganisatie te bevragen.

5 AANBEVELINGEN

5.1 Inleiding

Het ministerie van BZK neemt een algemene kaderstellende verantwoordelijkheid voor de informatieveiligheid van overheidsorganisaties. Een belangrijk onderdeel van deze verantwoordelijkheid is gericht op de werking van de bestaande informatieveiligheidsregels. Het is daarom zinvol voor het ministerie van BZK om overzicht en inzicht te krijgen in alle informatieveiligheidsregels die voor Nederlandse overheidsorganisaties gelden. Een dergelijk overzicht moet niet alleen vermelden waar regels staan, maar ook hoe ze zijn opgesteld, welke regelgevingspatronen er zichtbaar zijn en hoe deze regels uitpakken in de praktijk.

Om tot een dergelijk overzicht en inzicht te komen, heeft het ministerie van BZK aan Berenschot en VKA de opdracht gegeven om onderzoek te doen op basis van twee onderzoeksvragen:

1. Onderzoek bestaande wet- en regelgeving kaderstelling vanuit de rijksdienst en vanuit medeoverheden;
2. Onderzoek bestaande problemen bij de uitwisseling van informatie binnen en tussen overheidslagen en met aan de overheid gelieerde organisaties.

Het inzicht in de regels voor informatieveiligheid van overheidsorganisaties dient om een nadere onderbouwing te leveren voor een integraal afwegingskader (IAK) Informatieveiligheid. Dit IAK wordt vervolgens gebruikt om te bepalen waarmee de informatieveiligheid bij bestuursorganen gediend is. Naast het geven van overzicht en inzicht bevat dit rapport ook aanbevelingen voor de manier waarop het ministerie van BZK haar verantwoordelijkheid voor het regelgevend kader kan invullen.

In dit laatste hoofdstuk worden de bevindingen samengevat (paragraaf 5.2) en op basis daarvan een viertal aanbevelingen gedaan (paragraaf 5.3).

5.2 Samenvattende bevindingen

Op basis van de analyses uit de hoofdstukken 2-4, die volgden uit de 112 documenten uit de bijlage en een twaalf (groeps-) interviews, zijn een aantal samenvattende bevindingen te formuleren als antwoord op de onderzoeksvraag.

5.2.1 Een typologie van informatieveiligheidsregels (hoofdstuk 2)

Een analyse van de informatieveiligheidsregels voor overheidsorganisaties leidt tot de volgende typeringen. Informatieveiligheidsregels zijn in te delen in drie categorieën: inhoudelijke regels, regels over verantwoording en governance en toepassingsregels.

1. Regels betreffende de **inhoudelijke** eisen aan informatiebeveiliging. Dit zijn regels die zien op:
    a. vertrouwelijkheid, waaronder
        1. authenticatie;
        2. identificatie;

3. gegevensdeling;
4. autorisatie;

b. beschikbaarheid;
c. integriteit.

2. Regels betreffende de **toepassing** van de inhoudelijke eisen (wanneer zijn de regels op wie van toepassing?). Dit zijn regels die zien op:
   a. wie de regel van toepassing is;
   b. de omstandigheden waaronder de regel van toepassing is (rechtsfeit);
   c. de plaats waar de regel van toepassing is;
   d. de tijd waarop de regel van toepassing is.

3. Regels betreffende **toezicht, handhaving, verantwoording en governance** (eventueel ook: certificering). Dit zijn regels die zien op:
   a. functionele verantwoording;
   b. democratische verantwoording;
   c. toezicht en handhaving;
   d. sanctionering;
   e. certificering;
   f. governance.

5.2.2 Regelgevende patronen (hoofdstuk 2 en 3)

Met de categorisering van de regels en het overzicht van manieren waarop deze regels gesteld worden, zijn een aantal regelgevende patronen waar te nemen.

- Het toepassingsbereik van informatieveiligheidsregels wordt in de meeste gevallen bepaald door de aard van de te beveiligen gegevens. Een informatieveiligheidsregel is - meestal - gekoppeld aan de aard van de gegevens en niet aan de aard van het bestuursorgaan.
- Het geheel van informatieveiligheidsregels biedt de verschillende overheidsorganisaties in het sociale, fysieke en veiligheidsdomein veel ruimte om zelf de manier van regels stellen te bepalen.
- Als van informatieveiligheidsregels kiezen voor open normen wordt dat vaak gecombineerd met verwijzingen naar ISO en NEN standaarden.
- In een sector waarin een duidelijk gedeeld belang is en alle partijen tot de overheid behoren (zoals de watersector), is meer sprake van zelfbinding dan in sectoren waarin private en publieke partijen met verschillende belangen samenwerken.
- Opstellers kiezen voor bestuurlijke en operationele afspraken wanneer er geen noodzaak tot afdwingbaarheid gevoeld wordt.
- De relatie tussen informatieveiligheidsregels en de ketensamenwerkingen hangt af van de aard van de keten. Vooral ketens tussen verschillende bestuursorganen (publiek-publiek) en publiek-private ketens lopen een verhoogd risico op juridische knelpunten.

- Er zijn grote verschillen in de regels over toezicht en handhaving van informatieveiligheidsregels. Opstellers van regelgeving kiezen voor wettelijke verplichtingen wanneer er een noodzaak is om informatieveiligheidseisen af te dwingen. Meestal hangt deze noodzaak samen met de aard van de te beveiligen informatie. Vooral bijzondere persoonsgegevens en essentiële informatie krijgt in dat kader de aandacht.
- De inwerkingtreding van de AVG en vooral de afdwingbaarheid van de AVG heeft geleid tot relatief veel aandacht voor de bescherming van persoonsgegevens. De bescherming van niet-persoonsgegevens heeft minder aandacht van opstellers van informatieveiligheidsregels.
- Er is een inverse relatie tussen wettelijke producteisen en informatieveiligheidsregels. Naarmate de wettelijke producteisen een hogere garantie bieden op de informatieveiligheid van een product, is er minder noodzaak voor informatieveiligheidsregels.

5.2.3 Praktijkobservaties (Hoofdstuk 4)

Naast een typologie van informatieveiligheidsregels en regelgevende patronen is ook onderzoek gedaan naar de impact van de informatieveiligheidsregels in de praktijk. Daaruit zijn drie praktijkobservaties gedestilleerd:

1. Hoe informatieveiligheidsregels ook zijn opgesteld, ze worden altijd vertaald naar processen en producten die professionals helpen om compliant te zijn.
2. Overheidsorganisaties die met een grote verscheidenheid aan informatieveiligheidsregels te maken hebben, beoordelen vanuit efficiencyoverwegingen niet of informatiesystemen aan alle regels voldoen, maar controleren compliance aan informatieveiligheidsregels wanneer daar aanleiding voor is.
3. In ketensamenwerkingen worden informatieveiligheidseisen gesteld, maar er wordt weinig ingezet op het controleren van de naleving van deze eisen.

5.3 Vier aanbevelingen

Op basis van het onderzoek en de gedane bevindingen wordt BZK vier aanbevelingen gedaan ten aanzien van (het opstellen van) informatieveiligheidsregels voor overheden.

5.3.1 Aanbeveling I: richt de beleidsinspanningen op het stimuleren (bij positieve) of tegengaan (bij negatieve) van regelgevende patronen die bij het opstellen en toepassen van informatieveiligheidsregels zijn ontstaan

Het ministerie van BZK neemt een algemene verantwoordelijkheid voor de werking van het regelgevend kader voor informatieveiligheidsregels voor overheidsorganisaties. Dit ziet voor het merendeel op regels die BZK zelf niet heeft gesteld en waar het ministerie van BZK ook niet zelf over gaat. Het ligt daarom voor de hand om de beleidsinspanningen te richten op het stimuleren van positieve regelgevende patronen en het tegengaan van negatieve regelgevende patronen bij andere overheidsorganen. Deze patronen doen zich voor op Rijks-, provinciaal, gemeentelijk en

waterschapsniveau en in alle overheidssectoren. Bij het richten van de beleidsinspanningen moet met de verschillen tussen overheidslagen en overheidssectoren rekening gehouden worden.

Drie voorbeelden om deze aanbeveling te concretiseren zijn:

- Alle overheidslagen hebben zich gecommitteerd aan de Baseline Informatiebeveiliging Overheid (BIO). Deze koppeling biedt kansen voor informatieveiligheidsregels, bijvoorbeeld door in de Aanwijzingen voor de Regelgeving een aanwijzing over het verwijzen naar de BIO op te nemen. Ook is het mogelijk om overheidspartijen te stimuleren om een verwijzing naar de BIO in ketenafspraken (bijvoorbeeld convenanten) op te nemen.
- De inwerkingtreding van de AVG heeft geleid tot relatief veel aandacht voor de bescherming van persoonsgegevens in vergelijking met de bescherming van niet-persoonsgegevens. Overwogen kan worden om de beleidsinspanningen te richten op het vergroten van de aandacht voor de bescherming van niet-persoonsgegevens.
- Verzamel *best practices* en stimuleer dat opstellers van informatieveiligheidsregels deze toepassen bij het vaststellen van informatieveiligheidsregels.

5.3.2 Aanbeveling II: Mede bepalend voor de noodzaak voor het stellen van informatieveiligheidseisen is de mate waarin producteisen en de regelgeving rond bescherming van persoonsgegevens hierin al voorzien. Zoek daarom bij het reguleren de verbinding met de departementen die verantwoordelijk zijn voor producteisen (EZ) en de bescherming van persoonsgegevens (JenV). Onderzoek ook de Europese mogelijkheden.

Voor de werking zijn niet alleen de informatieveiligheidsregels relevant, maar ook op de verhouding van deze regels met aanpalende wetgeving. Voor twee aanpalende wetgeving geldt bovendien dat ze veel impact hebben op de noodzaak om informatieveiligheidsregels te stellen. Het betreft de wetgeving over producteisen en het wetgeving voor de bescherming van persoonsgegevens.

De mate waarin informatieveiligheidseisen aan producten zijn gesteld, is zeer relevant voor de informatieveiligheidseisen (die zien op processen). Zeker met de opkomst van de IoT is het steeds belangrijker deze samenhang in beeld te hebben. Daarbij geldt dat producteisen, vanwege de harmoniserende kracht van de Europese interne markt, vaak op Europees niveau gesteld worden en dat de beleidsverantwoordelijkheid voor dit onderwerp bij het ministerie van Economische Zaken en Klimaat (ministerie van EZK) belegd is. Om in samenhang op te trekken voor goede informatieveiligheidsregels is nauw contact met het ministerie van EZK noodzakelijk, zeker wanneer in Brussel onderhandeld wordt over producteisen die aan informatiebeveiliging raken.

De wetgeving voor de bescherming van persoonsgegevens heeft ook veel invloed op de kaderstellende verantwoordelijkheid van het ministerie van BZK. Deze invloed volgt uit de ontwikkeling die het regelgevend kader voor de bescherming van persoonsgegevens heeft doorgemaakt. De komst van de AVG is daarvan het meest zichtbare voorbeeld. Net als voor

producteisen geldt dat de bescherming van persoonsgegevens een Europese dimensie heeft en bovendien bij een ander ministerie (Justitie en Veiligheid - JenV), belegd is. Nauw contact met dit departement is daarmee ook in het belang van goede informatieveiligheidsregels.

Nu producteisen en de bescherming van persoonsgegevens een Europese dimensie kennen, ligt het voor de hand om ook te onderzoeken of iets dergelijks voor informatieveiligheidsregels ook nuttig is. Alleen op dat niveau is optimale aansluiting bij de aanpalende wetgeving goed mogelijk. Het verdient aanbeveling om op dit niveau de verbinding te zoeken.

5.3.3 Aanbeveling III: faciliteer dat overheidsorganisaties op een eenvoudige manier informatieveiligheidsregels onderdeel kunnen maken van ketenafspraken. Richt de aandacht daarbij op ketens tussen bestuursorganen (publiek-publiek) en publiek-private ketens (niet op ketens binnen één bestuursorgaan).

De laatste jaren ontstaat steeds meer publiek-publieke en publiek-private samenwerkingsverbanden. Voor overheidsorganisaties zijn deze samenwerkingen een instrument om publieke waarde te realiseren. Deze samenwerkingen zijn zichtbaar in alle overheidssectoren en binnen alle overheidslagen. Binnen deze samenwerkingen is de uitwisseling van informatie een voorwaarde voor het slagen van de samenwerking.

Aan publiek-publieke samenwerkingsverbanden ligt vaak een (al dan niet bindende) overeenkomst ten grondslag. Zodra informatie-uitwisseling onderdeel is van de samenwerking, ontstaat er een goede reden om informatieveiligheidsregels onderdeel te maken van de afspraken. Het ministerie van BZK, dat verantwoordelijkheid neemt voor het vaststellen van de minimumeisen binnen het regelgevend kader voor informatiebeveiliging, kan met standaardbepalingen eraan bijdragen dat informatieveiligheid een goede plaats in deze afspraken krijgt. Daarbij ligt een verbinding met de BIO voor de hand.

Aan publiek-private samenwerking ligt meestal een bindende overeenkomst ten grondslag. Net als voor publiek-publieke samenwerkingen zijn standaardbepalingen over informatiebeveiliging voor publiek-private samenwerkingen aanbevelingswaardig. In vergelijking met publieke samenwerkingen, moeten er in de standaardbepalingen extra aandacht zijn voor afdwingbare regels over toezicht, handhaving en sanctionering.

Stelsels die binnen één bestuursorgaan vallen (denk aan de diensten van Justitie en Veiligheid binnen de strafrechtketen), vallen onder de verantwoordelijkheid van dat ene bestuursorgaan. Het ministerie van BZK kan in deze gevallen *best practices* over de informatieveiligheidseisen in ketens delen, maar kan uit hoofde van haar kaderstellende en aanjagende rolde aandacht beter richten op andere ketens.

5.3.4 Aanbeveling IV: steek de verbetering van de informatieveiligheidsregels in vanuit het vereenvoudigen van de complexiteit aan regelgeving die CISO's en andere

informatieveiligheidsprofessionals moeten maken om hun collega's in het primaire proces in staat te stellen op een effectieve manier te opereren.

Mocht het ministerie van BZK zelf nadere regels willen gaan stellen om het juridisch kader voor informatiebeveiliging te verbeteren, dan wordt aanbevolen dat die regels zich richten op de praktijk van de mensen die binnen deze organisaties met die taak belast zijn, zoals CISO's en andere informatieprofessionals. Door bijvoorbeeld het nastreven van meer harmonisatie of verduidelijking in de veelheid aan regels te scheppen kunnen zij beter deze informatieveiligheidsregels gebruiken om slimme informatiebeveiligingsproducten te kiezen en heldere instructies voor de medewerkers uit te werken. Voorbeeld hiervan is het voorschrijven van het gebruik van veilig e-mailen of standaarden rondom identificatie van gebruikers. Er zijn een aantal gemeenschappelijke vraagstukken die voor bij alle overheidsorganisaties een rol spelen binnen informatieveiligheid, juist op die onderwerpen kunnen wettelijke voorschriften conflicteren.

Een andere mogelijkheden in de uitwerking ervan is het voorkomen van meer regels die de complexiteit vergroten of het zoveel mogelijk vereenvoudigen. Bijvoorbeeld door scherp te kijken naar de vitaal verklaringen, wettelijke verplichtingen en het toestaan van nieuwe (sector)regelgeving.

Daarbij verdient de positie van gemeenten, die in alle domeinen actief zijn en door de decentralisaties steeds meer informatie verzamelen en delen, extra aandacht. Het vereenvoudigen van de juridische complexiteit is wellicht mogelijk door met experimenteerbepalingen mogelijkheden te creëren om regelgeving buiten werking te stellen. Wanneer verschillende wetten op de werkvloer strijdige of onwerkbare eisen opleveren kan een dergelijke bepaling oplossing bieden door ruimte te geven om af te wijken wanneer bijvoorbeeld een risico-inschattingen wordt gedaan en bestuurlijke goedkeuring is verleend. De BIO geeft hiertoe al een aanzet met de risico-klassering maar heeft voor het overige nog niet de benodigde rechtgevende kracht om complexiteit te voorkomen.

BIJLAGE A: DE ONDERZOCHTE INFORMATIEVEILIGHEIDSREGELS

Deze bijlage bevat een overzicht van alle regels over informatiebeveiliging. Om alle regels zo overzichtelijk mogelijk weer te geven, zijn een aantal keuzes gemaakt:

1. Er is gekozen om de regels over informatiebeveiliging op documentniveau weer te geven. Het overzicht is dus een opsomming van documenten, niet van alle regels die deze documenten bevatten.
2. De documenten die regels bevatten hebben een verschillende status en naam. Het betreft bijvoorbeeld verdragen, verordeningen, richtlijnen, wetten, algemene maatregelen van bestuur en regelingen, maar ook beleidsregels, ISO-standaarden en andere normenkaders.
3. Van de belangrijkste documenten wordt ook een indicatie van de inhoud gegeven. Van minder belangrijke documenten wordt alleen aangegeven welke onderdelen of bepalingen regels over informatiebeveiliging bevatten.
4. Bij Europese regelgeving is gekozen om verordening zelfstandig weer te geven en daarbij relevante nationale wetten te noemen en voor richtlijnen slechts benoemen in welke wet ze zijn omgezet. Voor verdragen is ook gekozen om de wetten te benoemen waarin ze zijn omgezet, tenzij er geen goedkeuringswet voorhanden is (geldt bijvoorbeeld voor de NAVO-overeenkomst inzake uitwisseling van technische gegevens voor defensiedoeleinden, Brussel, 19 oktober 1970).
5. Veel overheidsorganisaties hebben ervoor gekozen om regels over informatiebeveiliging te stellen in convenanten, bestuursovereenkomsten en andere documenten. Deze categorie van regelstellen wordt alleen in algemene zin weergegeven.
6. De onderzoekers hebben al deze documenten bekeken en hebben op basis daarvan een analyse gemaakt over de manier waarop regels over informatiebeveiliging worden gesteld aan overheden. De weerslag van deze analyse staat in Hoofdstuk 2 van deze bijlage.

INHOUDSOPGAVE OVERZICHT INFORMATIEVEILIGHEIDSREGELS

1	**Wettelijke kernregels over informatieveiligheid**	**31**
1.1	Verdragen en overige regulering NAVO & EU	31
1.2	Algemene Verordening Gegevensbescherming (AVG)	31
1.3	Wet Beveiliging Netwerk- en Informatiesystemen (Wbni)	32
1.4	De Wet digitale overheid (Wdo) en de eIDAS-Verordening	33
1.5	Regels binnen de strafrechtketen (opsporingsinstanties, het openbaar ministerie en de rechter)	33
1.6	Overzicht van onderzochte wettelijke regels (inclusief bovenstaande)	35
2.	**Niet-wettelijke kernregels informatieveiligheid**	**40**
2.1	Overheidsbrede niet-wettelijke kernregels	40
2.1.1	Baseline Informatiebeveiliging Overheid (BIO)	40
2.1.2	Nederlandse Overheid Referentie Architectuur (NORA)	40
2.2	Voorschriften voor het Rijk	40
2.2.1	Voorschrift Informatievoorziening Rijksdienst (VIR 2007)	40
2.2.2	Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)	42
2.3	Voorschriften voor gemeenten (Eenduidige Normatiek Single Information Audit (ENSIA)	42
2.4	Standaarden	42
2.4.1	ISO 27001 en ISO 27002 e.v.	42
2.4.2	NEN 7510 e.v.	43
2.5	Sectorale uitwerkingen	43
2.5.1	Suwinet	44
2.6	Overige gezaghebbende vormen van instructies en regelingen	44
2.6.1	Adviezen NCSC	44
2.6.2	Aansluitvoorwaarden DigiD	44
2.7	Overzicht van onderzochte documenten	44
Overige gezaghebbende vormen van instructies en regelingen		45

1 WETTELIJKE KERNREGELS OVER INFORMATIEVEILIGHEID

1.1 Verdragen en overige regulering NAVO & EU

Er zijn een aantal verdragen (vanuit verschillende verbanden) gesloten die raakvlakken hebben met overheidsgerelateerde informatieveiligheidsregels. Voor het bereiken van verschillende doelstellingen (zoals EU-doelstellingen en NAVO-doelstellingen) zijn afspraken gemaakt om effectief politiek overleg, samenwerking en planning te bereiken en de uitwisseling van gerubriceerde informatie tussen partijen mogelijk te maken. Ook zijn er afspraken gemaakt op verdragsniveau of ter bestrijding van cybercriminaliteit. Deze afspraken zijn (indirect) terug te vinden in de overheidgserelateerde afspraken rondom informatieveiligheid, o.a. ten aanzien van de rubricering en verstrekking ervan. Daarnaast gelden er binnen de Raad voor de EU ook besluiten die zien op de veiligheid van informatie en rubricering daarvan.

Belangrijkste gelieerde regelgeving

Besluit van de Raad betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (Besluit van de Raad, 23 september 2013 2013/488/EU), vaak in het Engels naar gerefereerd als 'Council security rules for protecting classified information (EUCI).	Dit besluit heeft tot doel een alomvattend beveiligingssysteem voor de bescherming van gerubriceerde informatie op te zetten dat de Raad van de EU, zijn secretariaat-generaal (SGR) en de EU-landen bestrijkt, ter ondersteuning van de activiteiten van de Raad op alle gebieden waarvoor de verwerking van gerubriceerde informatie vereist is. In het besluit worden de grondbeginselen en minimumnormen voor de beveiliging van gerubriceerde EU-gegevens (EUCI) vastgesteld. Deze beginselen en normen zijn van toepassing op de Raad en het secretariaat-generaal en moeten door de EU-landen overeenkomstig hun wetgeving worden nageleefd om ervoor te zorgen dat elk land een gelijkwaardig niveau van bescherming biedt als EUCI. Daardoor heeft deze regelgeving ook impact op de bescherming bij gegevensuitwisseling met andere landen.

1.2 Algemene Verordening Gegevensbescherming (AVG)

Relevantie voor dit onderzoek

Veel informatiesystemen van de overheid bevatten persoonsgegevens. Op de bescherming van deze persoonsgegevens is de AVG van toepassing. De AVG verplicht verwerkingsverantwoordelijken tot het treffen van passende technische en organisatorische maatregelen ter bescherming en beveiliging van de gegevens (artikelen 24, 25 en 32, van de verordening). Veel bestuursorganen zijn verwerkingsverantwoordelijke en moeten daarom dit type informatie in lijn met de AVG beschermen.

Belangrijkste gelieerde regelgeving

Regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming)	Er zijn twaalf besluiten en regelingen op de uitvoeringswet gebaseerd.

1.3 Wet Beveiliging Netwerk- en Informatiesystemen (Wbni)

Relevantie voor dit onderzoek

Deze wet is een omzetting van de NIB-richtlijn. Deze richtlijn is erop gericht om het niveau van netwerk- en informatiebeveiliging in Europa gelijk te trekken. In de Wbni worden daartoe “aanbieders van essentiële diensten” en “digitale dienstverleners” aangewezen waarop de wet van toepassing is. Onder deze normadressaten vallen ook overheidsorganisaties.

Belangrijkste gelieerde regelgeving

Europese Netwerk- en Informatiebeveiliging (NIB) richtlijn 2016 / 1148	Deze richtlijn is omgezet in de Wbni. De Wbni bevat overigens een groot aantal dynamische verwijzingen naar NIB.
EU Cybersecurity act 2019/881	Deze verordening regelt de oprichting van ENISA. Deze Europese organisatie is gericht op de correcte implementatie van richtlijn 2016/1148 en hangt nauw samen met de Wbni.
Lagere regelgeving	Er zijn vier besluiten op deze wet gebaseerd.

1.4 De Wet digitale overheid (Wdo) en de eIDAS-Verordening

Relevantie voor dit onderzoek

Het voorstel voor de Wet digitale overheid is op dit moment (23 oktober 2019) in behandeling bij de Tweede Kamer. Het vormt een eerste tranche van regelgeving voor de verdere digitalisering van de overheid. Indien de Wdo wordt aangenomen door de Staten-Generaal heeft ze een grote impact op de informatieveiligheidsregels voor de overheid. Zo bevat het wetsvoorstel van de regering een grondslag om in lagere regelgeving regels te stellen “met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten op verschillende betrouwbaarheidsniveaus”.

De Wdo en de eIDAS-verordening (inclusief uitvoeringsverordeningen op basis van de eIDAS verordening) kennen veel raakvlakken. Waar de Wdo geldt voor elektronische diensten in Nederland, is de eIDAS verordening van toepassing op grensoverschrijdende authenticatie voor burgers en bedrijven. Vanwege deze verwantschap bevat de Wdo verschillende verwijzingen naar eIDAS verordening.

De Europese eIDAS verordening is echter al in werking getreden (op 29 september 2018). Vanaf dat moment moeten publieke organisaties en private organisaties met een publieke taak Europees erkende inlogmiddelen accepteren binnen de digitale dienstverlening. Deze verplichting geldt o.a. voor organisaties die gebruik maken van DigiD en eHerkenning.

Belangrijkste gelieerde regelgeving

Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten)	De eIDAS-verordening werkt rechtstreeks, maar vereiste ook dat nationale wetgeving in lijn werd gebracht.

1.5 Regels binnen de strafrechtketen (opsporingsinstanties, het openbaar ministerie en de rechter)

Relevantie voor dit onderzoek

De informatieveiligheidsregels binnen de strafrechtketen verdienen bijzondere aandacht.

- Voor het **openbaar ministerie** is de Wet justitiële en strafvorderlijke gegevens (Wjsg) relevant. In de Wiggen staan waarborgen voor een zorgvuldige omgang met strafvorderlijke gegevens door het Openbaar Ministerie. Daaronder vallen ook informatieveiligheidsregels.
- Voor de **opsporingsinstanties** is de Wet politiegegevens (Wpg) van belang. De Wpg regelt de verwerking van persoonsgegevens voor de uitoefening van de politietaak door politie (waaronder de Rijksrecherche), de Koninklijke marechaussee, de bijzondere opsporingsdiensten Fiscale Inlichtingen- en Opsporingsdienst,/Economische Controledienst (FIOD-ECD), de Inspectie Sociale Zaken en Werkgelegenheid (ISZW)-directie opsporing, de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport (ILT-IOD) en de Inlichtingen- en Opsporingsdienst van de nieuwe Voedsel en Waren Autoriteit (VWA-IOD). De Wpg (en onderliggende regelgeving) bevatten informatieveiligheidsregels.
- Voor de **rechtelijke instanties** is de Wet op de rechterlijke organisatie, het Wetboek van Burgerlijke Rechtsvordering en het wetboek van Strafvordering van belang. De informatieveiligheidsregels staan overigens in lagere regelgeving (onder meer Besluit digitale stukken Strafvordering en diverse amvb's voor de burgerlijke rechtsvordering, zie verder overzicht onder overig).

Belangrijkste gelieerde regelgeving

Richtlijn gegevensbescherming opsporing en vervolging (EU 2016/680)	Deze richtlijn in omgezet in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens met het wetvoorstel Wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen (kamerstuk 34 889).
Cybercrimeverdrag (2001) en latere protocollen.	Dit verdrag is omgezet in het Wetboek van Strafrecht en het Wetboek van Strafvordering. Zie tweede nota van wijziging van het wetsvoorstel Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II) (kamerstuk 26 671, nr. 7)
Onderliggende regelgeving	

1.6 Overzicht van onderzochte wettelijke regels (inclusief bovenstaande)

Dit is geen volledig overzicht van alle documenten met informatieveiligheidsregels. Dit zijn de documenten met informatieveiligheidsregels die onderdeel waren van dit onderzoek.

Document	Relevante bepalingen (art.)
Verdragen en breder werkende EU besluiten	
1. NAVO-overeenkomst inzake uitwisseling van technische gegevens voor defensiedoeleinden, Brussel, 19 oktober 1970	Zie toelichting hierboven
2. 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.	Zie toelichting hierboven
3. Cybercrimeverdrag (2001) en latere protocollen	Zie toelichting hierboven
4. Besluit van de Raad betreffende de beveiligingsvoorschriften voor de bescherming van gerubriceerde EU-informatie (EUCI), (2013/488/EU)	Zie toelichting hierboven
EU-verordeningen en richtlijnen	
1. Algemene Verordening Gegevensbescherming	Zie toelichting hierboven
2. NIB-richtlijn	Zie toelichting hierboven
3. eIDAS Verordening	Zie toelichting hierboven
4. Richtlijn gegevensbescherming opsporing en vervolging	Zie toelichting hierboven
5. EU Cybersecurity act 2019/881	Zie toelichting hierboven
6. Verordening (EU) 2018/1807 van het Europees Parlement en de Raad van 14 november 2018 inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens in de Europese Unie.	6
7. Verordening (EU) 2019/1155 van het Europees Parlement en de Raad van 20 juni 2019 tot wijziging van Verordening (EG) nr. 810/2009 tot vaststelling van een gemeenschappelijke visumcode (Visumcode)	44, derde lid
8. Verordening (EU) nr. 1285/2013 van het Europees Parlement en de Raad van 11 december 2013 betreffende de uitvoering en exploitatie van de Europese satellietnavigatiesystemen en tot intrekking van Verordening (EG) nr. 876/2002 van de Raad en Verordening (EG) nr. 683/2008 van het Europees Parlement en de Raad	17 en 21

9. Besluit nr. 1104/2011/EU van het Europees Parlement en de Raad van 25 oktober 2011 betreffende de voorwaarden voor toegang tot de overheidsdienst (publiek gereguleerde dienst) die wordt aangeboden door het wereldwijde satellietnavigatiesysteem dat is ingevoerd door het Galileo-programma	4
Wetten	
1. Uitvoeringswet Algemene verordening gegevensbescherming	Meerdere bepalingen
2. Wet Beveiliging Netwerk- en Informatiesystemen	Meerdere bepalingen
3. Wet digitale overheid	Meerdere bepalingen
4. Wet justitiële en strafvorderlijke gegevens	Meerdere bepalingen
5. Wet politiegegevens	Meerdere bepalingen
6. Wet op de rechterlijke organisatie	23 en 91
7. Wetboek van Strafvordering	Enkele grondslagen voor amvb's
8. Wetboek van Burgerlijke Rechtsvordering	Enkele grondslagen voor amvb's
9. Algemene wet bestuursrecht	8:36f
10. Wet bescherming staatsgeheimen	
11. Archiefwet	
12. Politiewet 2012	23
13. Telecommunicatiewet	18.2
14. Wet veiligheidsregio's	21
15. Wet op de inlichtingen- en veiligheidsdiensten 2017	24
16. Wet publieke gezondheid	24, 25
17. Wet veiligheidsonderzoeken	(vanwege vermelding in BIO)
18. Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI)	73, vijfde lid
19. Wet basisregistratie personen (Wet BRP)	1.10, 2.7,2.34, 2.37, 2.69, 2.77, 2.78, 3.1, 3.13 en 3.14
Lagere regelgeving (algemene maatregelen van bestuur)	
1. Besluit Jeugdwet	7.2.1 en 7.2.2

2. Besluit SUWI	5.22
3. Besluit betrouwbaarheid en vertrouwelijkheid elektronisch verzenden van verzoeken en mededelingen met betrekking tot de rol	1
4. Besluit digitale stukken Strafvordering	3
5. Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht	2
6. Besluit elektronische dienstverlening burgerlijke stand	1
7. Besluit elektronische gegevensverwerking door zorgaanbieders	alle bepalingen zijn relevant
8. Besluit elektronische indiening dagvaarding [Ingetrokken voor procedures en gerechten waarvoor digitaal procederen geldt]	3
9. Besluit informatie-uitwisseling bovengrondse en ondergrondse netten en netwerken	8
10. Besluit regels registratie elektronische adressen van derden en elektronisch betekenen in geval van derdenbeslag	2
11. Besluit ex artikel 24 Wet politiegegevens	
12. Besluit onderzoek in een geautomatiseerd werk	10
13. Besluit politiegegevens	Meerdere bepalingen
14. Besluit politiegegevens buitengewoon opsporingsambtenaren	Meerdere bepalingen
15. Besluit politiegegevens bijzondere opsporingsdiensten	Meerdere bepalingen
16. Besluit vaststelling nadere regels vastleggen en bewaren kentekengegevens ex artikel 126jj Wetboek van Strafvordering door politie	
17. Besluit verplichte politiegegevens	
18. Besluit verwerking persoonsgegevens bij selectieve woningtoewijzing ter beperking van overlast gevend en crimineel gedrag	
19. Besluit basisregistratie personen	Diverse bepalingen, waaronder 3,4,5, 6
Lagere regelgeving (ministeriële regelingen)	
1. Subsidiebesluit raad voor rechtsbijstand	8
2. Aanwijzingsbesluit beheerder bel-me-niet-register 2017–2019	5
3. Beheersregeling documentaire informatieverzorging Infrastructuur en Waterstaat	28

4. Bekendmakingsregeling	2
5. Besluit aandachtspunten voor de accountantscontrole Dienst Wegverkeer	2
6. Besluit aanwijzing exameninstellingen voor de binnenvaart 2017	4
7. PODACS-regeling	5
8. Raamregeling Telewerken	5
9. Regeling Informatiehuishouding Financiën 2016 (RINFIN2016)	22
10. Regeling SUWI	6.3, 6.4 en Bijlage I
11. Regeling Wet bescherming persoonsgegevens Ministerie van Financiën	4
12. Regeling aandachtspunten accountantscontrole OPTA	2
13. Regeling beveiliging nucleaire inrichtingen en splijtstoffen	Bijlage III
14. Regeling documentair informatiemanagement VWS 2015	28
15. Regeling elektronische bekendmaking Tractatenblad	2
16. Regeling elektronische bekendmaking en beschikbaarstelling regelgeving decentrale overheden	1
17. Regeling informatiebeveiliging politie	Alle bepalingen
18. Regeling informatievoorziening WPO/WEC	Bijlage I
19. Regeling justitiële keteninformatisering Jeugdwet	Bijlage 5
20. Regeling pseudonimisering onderwijsdeelnemers	5
21. Regeling publieke gezondheid	5
22. Regeling sturing van en toezicht op de Dienst Wegverkeer	5
23. Regeling sturing van en toezicht op de Luchtverkeersleiding Nederland	Bijlage bij artikel 6
24. Regeling sturing van en toezicht op de NIWO	Bijlage bij artikel 3
25. Regeling sturing van en toezicht op het Centraal Bureau Rijvaardigheidsbewijzen	5
26. Regeling sturing van en toezicht op het Kadaster	5
27. Regeling vaststelling LFNP	Bijlage 3
28. Regeling voorzieningen GDI	6
29. Regeling bestrijding schadelijke organismen	8
30. Regeling beoordeling reinigbaarheid grond 2006	1
31. Regeling bodemkwaliteit	Bijlage C

32. Regeling gebruik burgerservicenummer in de zorg	1
33. Regeling justitiële keteninformatisering Jeugdwet	Bijlage 5
34. Regeling publieke gezondheid	5
35. Regeling Jeugdwet	6
36. Regeling forensische zorg	3
37. Regeling particuliere beveiligingsorganisaties en recherchebureaus	20 en bijlage 6 en 23a
38. Regeling zorgverzekering	6.2.8, tweede lid, onder c
39. Regeling team criminele inlichtingen Inspectie SZW-DO	
40. Regeling team criminele inlichtingen FIOD	
41. Controleprotocol voor de jaarverantwoording politie	Bijlage I
42. Informatiestatuut Onafhankelijke Post en Telecommunicatie Autoriteit	12
43. Kaderregeling documentaire informatievoorziening Sociale Zaken en Werkgelegenheid 2014	7
44. Samenwerkingsregeling politie-Koninklijke marechaussee	1a
45. Uitvoeringsregeling Archiefbeheer Veiligheid en Justitie 2014	3
46. Uitvoeringsregeling verordening Europees burgerinitiatief	Bijlage 2
47. Uitvoeringsregeling Wmo 2015	3
48. Vervangingsbesluit BZ 2015	Bijlage als bedoeld in artikel 3
49. Regeling basisregistratie personen	Diverse bepalingen

2. NIET-WETTELIJKE KERNREGELS INFORMATIEVEILIGHEID

In dit hoofdstuk worden de niet-wettelijk kernregels informatieveiligheid opgesomd. Van een aantal wordt een nadere toelichting gegeven. In de laatste paragraaf staat een overzicht van alle gevonden niet-wettelijke kernregels.

2.1 Overheidsbrede niet-wettelijke kernregels

2.1.1 Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is een normenkader dat het resultaat is van verplichtende zelfregulering. Het is daarmee geen wettelijke norm, maar veronderstelt dat de verschillende overheidslagen zelf de verantwoordelijkheid nemen voor het maken van niet-vrijblijvende afspraken. Alle overheidslagen (Rijk, provincies, gemeenten en waterschappen) hebben de BIO overgenomen en vervangen daartoe de BIR (Rijk), IBI (provincie), BIG (gemeenten) en BIWA (waterschappen). De BIO is op 1 januari 2019 in werking getreden. De verschillende overheidslagen zijn op dit moment bezig de BIO te implementeren, door bijvoorbeeld het aanpassen van ENSIA (zie onder gemeenten).

2.1.2 Nederlandse Overheid Referentie Architectuur (NORA)

Op digitaleoverheid.nl staat NORA als volgt kernachtig omschreven: “NORA is begonnen als een set van afspraken om digitale dienstverlening in de publieke sector mogelijk te maken en te verbeteren. Nog steeds vormen de bindende afspraken over interoperabiliteit en kwaliteit van dienstverlening de kern van de NORA: 10 Basisprincipes en 38 Afgeleide Principes.”

De basisprincipes en afgeleide principes bevatten regels over informatieveiligheid. Een voorbeeld is basisprincipe 8 (afnemers kunnen erop vertrouwen dat informatie niet wordt misbruikt), met als beschrijving:

“de dienstverlener garandeert dat informatie alleen toegankelijk is voor bevoegde personen en alleen wordt gebruikt voor het doel waarmee zij is verzameld. Dit principe geldt niet alleen voor informatie over personen, maar ook voor informatie over bedrijven en de overheid zelf. Zo kunnen bedrijfsgegevens waaruit investeringsbeslissingen zijn af te leiden interessant zijn voor de concurrentie. Informatie over overheidsgebouwen kan interessant zijn voor terroristen.”

2.2 Voorschriften voor het Rijk

2.2.1 Voorschrift Informatievoorziening Rijksdienst (VIR 2007)

Het Voorschrift Informatievoorziening Rijksdienst (VIR 2007) is een besluit van de Minister-President, handelend in overeenstemming met een gevoelen in de Ministerraad. Het is een intern

werkend voorschrift dat informatieveiligheidsregels bevat voor de rijksdienst (waartoe gerekend worden de ministeries met de daaronder ressorterende diensten, bedrijven en instellingen).

De opstellers van de VIR 2007 kiezen ervoor om niet op het niveau van technische maatregelen regels op te stellen voor informatiebeveiliging. Als reden wordt de korte levenscyclus van informatietechnologieën genoemd: “een nieuwe technologie kan zijn intrede doen zonder dat daarover nu uitspraken mogelijk zijn en bestaande technologieën kunnen binnen een paar jaar verouderd zijn” (uit de toelichting VIR 2007).

Ook waar het gaat om organisatorische maatregelen is gekozen voor globale regels voor wat minimaal ministerie-breed geregeld dient te worden. Dit heeft geleid tot eisen aan informatiebeveiligingsbeleid (artikel 3) en een beschrijving van de verantwoordelijkheden van het lijnmanagement (artikel 4). Met het citeren van beide bepalingen, is direct de kern van VIR 2007 inzichtelijk. Deze regeling blijft van kracht naast de BIO voor de Rijksdienst.

Artikel 3
De secretaris-generaal van een ministerie stelt het informatiebeveiligingsbeleid vast, draagt dit uit en legt verantwoording hierover af. Het beleid bestaat uit:

a. De strategische uitgangspunten en randvoorwaarden die het ministerie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid;
b. De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden;
c. De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers;
d. De gemeenschappelijke betrouwbaarheidseisen en normen die op het ministerie van toepassing zijn;
e. De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd;
f. De bevordering van het beveiligingsbewustzijn.

Artikel 4
Het lijnmanagement is verantwoordelijk voor de beveiliging van zijn informatiesystemen. Het lijnmanagement:

a. Stelt op basis van een expliciete risico afweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;
b. Is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
c. Stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd;
d. Evalueert periodiek het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen en stelt deze waar nodig bij.

2.2.2 Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)

Het Voorschrift Informatiebeveiliging Rijksdienst - bijzondere informatie (VIR-BI) geeft regels voor de beveiliging van gerubriceerde informatie bij de rijksdienst. De rijksdienst kent 4 niveaus gerubriceerde informatie: Departementaal Vertrouwelijke informatie (DepV) en 3 varianten staatsgeheime informatie (STG Zeer Geheim, Geheim en Confidentieel). Deze regels strekken er toe het aantal personen dat met gerubriceerde informatie in aanraking komt zo beperkt mogelijk te houden (het "need to know" principe). Ook moeten voldoende maatregelen worden genomen, bijvoorbeeld versleuteling van de informatie, om te voorkomen dat externe partijen toegang tot staatsgeheime informatie kunnen krijgen. Alleen gescreende medewerkers krijgen toegang tot Staatsgeheimen. Daarnaast is het van belang dat zo spoedig mogelijk actie wordt ondernomen bij kennisname door niet gerechtigden (compromitteren). De beveiligingsambtenaar (BVA) speelt hierbij een centrale rol. Voor het rubriceren van bijzondere informatie is een Handleiding Rubricering opgesteld.

2.3 Voorschriften voor gemeenten (Eenduidige Normatiek Single Information Audit (ENSIA)

Op digitaleoverheid.nl staat ENSIA als volgt kernachtig omschreven: "ENSIA is ontstaan vanuit een gezamenlijk initiatief van de ministeries Binnenlandse Zaken en Koninkrijksrelaties, (voormalig) ministerie van Infrastructuur en Milieu, Sociale Zaken en Werkgelegenheid en de Vereniging van Nederlandse Gemeenten (VNG). Met als doel te komen tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatiebeveiliging."

Belangrijk in de ENSIA systematiek is het onderscheid tussen horizontale en verticale verantwoording. De horizontale (democratische) verantwoording bestaat uit de zelfevaluatie, een IT-audit, een verklaring van het College van B&W en een passage over informatieveiligheid in het jaarverslag. De verticale (functionele) verantwoording ziet op de verantwoording over de informatiestelsels Basisregistratie Personen (BRP, Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet).

Belangrijk uitgangspunt van ENSIA is de single information audit. Dit betekent dat gemeenten zich in één keer over alle informatieveiligheidseisen verantwoorden via ENSIA.

2.4 Standaarden

2.4.1 ISO 27001 en ISO 27002 e.v.

ISO 27001 en ISO 27002 zijn internationale normenkaders voor de beveiliging van informatie(systemen) bij de overheid.

NORA omschrijft ISO 27001 als volgt: "ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een

gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden."

NORA omschrijft ISO 27002 als volgt: "ISO 27002 'Code voor informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid."

De eerdergenoemde Baseline Informatiebeveiliging Overheid (BIO) is gebaseerd op ISO 27001 en 27002.

2.4.2 NEN 7510 e.v.

NEN 7510 is door het Nederlands Normalisatie-Instituut ontwikkeld voor informatiebeveiliging in de zorg. NEN 7510 schrijft voor hoe een organisatie informatie kan beveiligen maar kent zelf geen uitgewerkte technische maatregelen. NEN 7510 is zowel geschikt voor overheidsorganisaties binnen de zorg als voor zorgpartijen die niet bij de overheid horen. Naast de NEN 7510 zijn er ook nadere uitwerkingen te vinden in de NEN 7512 en 7513.

NEN 7510 is een managementsysteem die een kader stelt voor het organiseren en borgen van informatiebeveiliging binnen een zorginstelling of toeleverancier. NEN7512 en NEN 7513 zijn aanvullingen op specifieke eisen uit de NEN 7510.

NEN 7510 en ISO 27001 zijn allebei normen die iets zeggen over hoe organisaties zouden kunnen/moeten omgaan met informatiebeveiliging. Het verschil tussen deze twee is dat de NEN 7510 is toegespitst op de zorg. In de zorg is de privacy van cliënten afhankelijk van het handhaven van de vertrouwelijkheid van persoonlijke gezondheidsinformatie. Om deze vertrouwelijkheid te handhaven, moeten er ook maatregelen worden genomen voor het handhaven van de integriteit van gegevens. Daarnaast is een hoog beschikbaarheidsniveau ook een kenmerk van zorginformatiesystemen, waar behandelingen vaak afhankelijk zijn van tijd. Daarom gelden andere/aanvullende vereisten.

De NEN 7510:2017 bestaat uit twee delen. Deel 1 bevat de normatieve voorschriften voor het managementsysteem volgens ISO 27001. Deel 2 vormt de Nederlandse weergave van de Europese en mondiale normen uit ISO 27002 en ISO 27799 (zorgspecifiek). [9]

2.5 Sectorale uitwerkingen

[9] FAQ Werken met NEN7510 (www.nen.nl)

2.5.1 Suwinet

Binnen het domein werk en inkomen delen gemeenten, het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en de Sociale Verzekeringsbank (SVB), informatie in een gemeenschappelijk, virtueel dossier: het Digitaal Klantdossier (DKD). Via Suwinet delen deze partijen de gegevens voor het DKD.

Via Suwinet wordt veel en gevoelige informatie over W&I-cliënten gedeeld. Er is daarom ook veel aandacht voor de beveiliging van deze informatie. In het overzicht van wettelijke regelingen is dat ook zichtbaar (zie verwijzingen naar Wet SUWI, Besluit SUWI, Regeling SUWI). In aanvulling daarop is het Suwinet normenkader opgesteld. Verder is er een verbinding met ENSIA (zie hierboven).

2.6 Overige gezaghebbende vormen van instructies en regelingen

2.6.1 Adviezen NCSC

Gezaghebbende overheidsorganisaties zoals het NCSC geven adviezen die in de praktijk als 'standaarden' worden gehanteerd. In beginsel zijn dit vrijblijvende adviezen, maar wordt in praktijk al de manier gezien om algemene voorschriften nader technisch in te vullen. Vanuit de algemene (bestuurlijke) zorgplicht geldt het devies om adviezen van het NCSC op te volgen. Een voorbeeld hiervan is de gemelde zwakte in door overheidsorganisaties veel gebruikte VPN-oplossing. Het niet opvolgen van deze adviezen wordt in praktijk gezien als een verzuim van de zorgplicht.

2.6.2 Aansluitvoorwaarden DigiD

Wanneer een organisatie een bij wet vastgestelde publieke taak uitvoert, conform een wettelijke bepaling gerechtigd is het BSN te verwerken en DigiD wil gebruiken, kan deze organisatie Logius vragen om aangesloten te word op DigiD. Daarvoor moet deze organisatie de Aansluitvoorwaarden DigiD accepteren. Dit zijn geen wettelijk vastgelegde vereisten, maar vanuit Logius opgelegde afspraken die door het afdwingende karakter en het brede gebruik tot een standaard zijn geworden binnen overheidsorganisaties. Er is immers maar één aanbieder van een voorziening als DigiD, als organisatie heb je deze te accepteren. Ook deze voorwaarden bevatten instructies ten aanzien van de informatieveiligheid.

2.7 Overzicht van onderzochte documenten

Overheidsbreed	
1.	Baseline Informatiebeveiliging Overheid (BIO)
2.	Nederlandse Overheid Referentie Architectuur (NORA) principes en standaarden
Rijk	
1.	Voorschrift Informatievoorziening Rijksdienst (VIR 2007)
2.	Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)

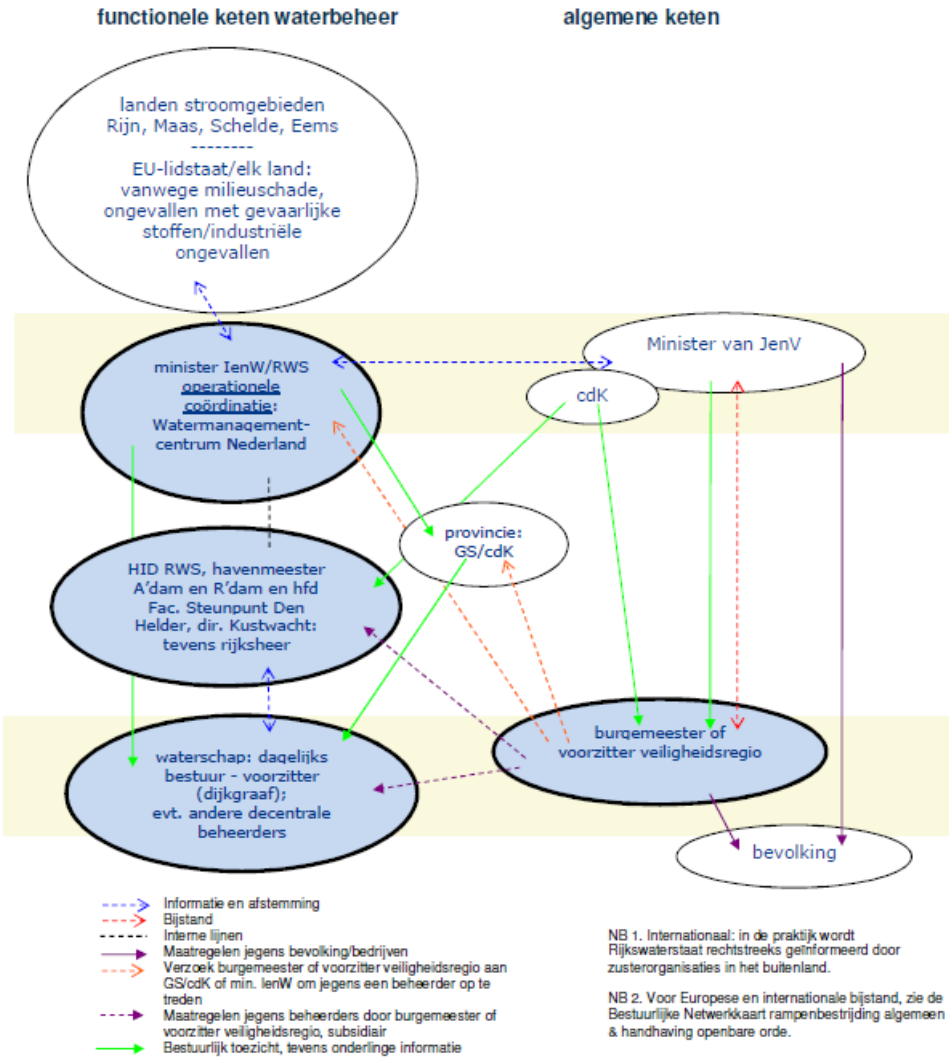
3. Algemeen Rijksambtenarenreglement (ARAR)
4. Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016)
5. Gedragsregeling voor de digitale werkomgeving (1 juli 2016; SGO besluit)
6. Het NKBR (Normenkader beveiliging Rijkskantoren) 2015
7. Kader Rijkstoegangsbeleid
Gemeente
1. Eenduidige Normatiek Single Information Audit (ENSIA)
Standaarden
1. NEN 7510 (ev)
2. ISO 27001
3. ISO 27002
Sectorale regels
Suwinet normenkader
Overige gezaghebbende vormen van instructies en regelingen
Adviezen NCSC
Aansluitvoorwaarden DigiD

BIJLAGE B: DE UITWERKING VAN TWEE PERSONAE

1.1 Personae I: Operational Security Officer bij een waterschap

INTRODUCTIE CASUS

Hans werkt als operational security officer (OSO) bij een waterschap. Binnen het waterschap is zijn rol het daadwerkelijk uitvoeren van technische beveiligingsmaatregelen bij het uitwisselen van waterstanden met andere ketenpartijen. Bij overstromingen en ernstige wateroverlast is de beschikbaarheid van informatie van het allergrootste belang. Bovendien moet deze informatie, indien nodig, met veel partners gedeeld kunnen worden. Deze uitwisseling van informatie is behoorlijk complex zoals deze bestuurlijke netwerkkaart crisisbeheersing laat zien.[10]



[10] Instituut fysieke veiligheid, IFV

BESCHRIJVING VAN HET REGELGEVEND KADER

Voor de beschrijving van het regelgevend kader waarbinnen Hans opereert, is het onderscheid tussen persoonsgegeven en overige gegevens erg belangrijk. In deze casus is Hans verantwoordelijk voor de uitwisseling van waterstanden. Voor de beschrijving van het regelgevend kader wordt ervan uit gegaan dat deze waterstanden geen persoonsgegevens bevatten.

Voor de informatiebeveiliging van deze niet-persoonsgegevens van waterschappen is geen sprake van uitgewerkte informatieveiligheidseisen in wetten, amvb's of regelingen. Ieder waterschap heeft strikt juridisch gezien een eigen verantwoordelijkheid om de informatiebeveiliging van niet-persoonsgegevens te regelen.

Dit betekent niet dat er geen afspraken zijn waar de waterschappen zich aan moeten houden. Deze hebben echter geen wettelijke status. Een belangrijk voorbeeld is het Bestuursakkoord water (BAW), dat voor het laatst is aangevuld in 2018.Dit is een akkoord tussen het Rijk, het Interprovinciaal Overleg (IPO), de Vereniging van Nederlandse Gemeenten (VNG), de Unie van Waterschappen (UvW) en de Vereniging van waterbedrijven in Nederland (Verwin). In de aanvulling uit 2018 staan onder meer "de kansen voor de informatiesamenleving" en de "risico's van digitale dreigingen" centraal. Het doel van deze samenwerking is onder meer:

> *dat data en informatie op orde zijn en dat informatie -ten behoeve van taakuitoefening en samenwerking - goed wordt ontsloten, door afspraken te maken over standaardisatie en afstemming. Met een verdere professionalisering, de noodzakelijke standaardisatie en meer open en uniforme ontsluiting van data zijn aanvullende efficiencyvoordelen te bereiken. Conform de Algemene Verordening Gegevensverwerking (AVG) werken de BAW-partners vanuit het principe van privacy en security by design.*

Over deze doelstelling staan een reeks afspraken genoemd. Deze afspraken zien op het maken van nadere afspraken over de interoperabiliteit, (open) data delen, standaarden toepassen, hergebruik van beschikbare toepassingen en het beveiligen van data.

Een ander voorbeeld van niet wettelijke zelfbinding is de Baseline Informatiebeveiliging Overheid (BIO). De waterschappen hebben zelf besloten om zich aan de BIO te binden, hetgeen in het BAW weer wordt bevestigd (pagina 15). De waterschappen gebruiken BAW en de BIO om de inspanningen voor de informatieveiligheid te richten.

Voor de uitwisseling van informatie binnen de keten (zie plaatje hierboven), zijn een aantal convenanten gesloten. In deze convenanten staan diverse voorwaarden waaraan het waterschap moet voldoen, om toegang te krijgen tot de informatie van de andere ketenpartners. Voor de uitwisseling van informatie over waterstanden zijn deze ketenpartner publieke organisaties.

DE VERHOUDING TUSSEN HET REGELGEVEND KADER EN HET DAGELIJKS WERK VAN HANS

In zijn dagelijks werk is Hans niet bezig met het regelgevende kaders en juridische regels. Hij is verantwoordelijk voor een goed functionerende uitwisseling van waterstanden tussen publieke ketenpartners. Daarbij hebben vooral de integriteit en beschikbaarheid van de informatie de aandacht. De vertrouwelijkheid is heeft minder aandacht: informatie over waterstanden is in beginsel openbare informatie.

De uitwisseling van waterstanden vindt plaats op basis van een convenant tussen Rijkswaterstaat en het waterschap. Opvallend is dat in dit convenant weinig concrete afspraken staan over de integriteit en beschikbaarheid van informatie. Hans geeft als verklaring dat zijn aandacht ligt bij de procesautomatisering om de uitwisseling van informatie mogelijk te maken en dat het belang van integriteit en beschikbaarheid zo voor de hand liggend is, dat extra regels stellen over integriteit en beschikbaarheid van die informatie niet noodzakelijk is.

MOGELIJKE JURIDISCHE KNELPUNTEN

In het algemeen zijn er geen juridische knelpunten. Hans wordt in zijn werk als OSO die verantwoordelijk is voor de waterstanden weinig geconfronteerd met regels van buiten. Als er al regels van buiten komen, zijn dit operationele en bestuurlijke afspraken (zie kwadrant hoofdstuk 2) waarmee het waterschap zelf heeft ingestemd (BAW, BIO en convenanten). Deze afspraken vertaalt het waterschap naar de eigen interne procedures. Dit geldt voor de inhoudelijke regels, het regels over toepassingsbereik en de verantwoordingsregels.

In theorie kan er een knelpunt ontstaan in de ketenafspraken. Zo is het mogelijk dat een ketenpartner alleen waterstanden wil uitwisselen als het waterschap voldoet aan informatieveiligheidseisen die botsen met de processen van het waterschap. Hiervan lijkt in de praktijk weinig sprake. Binnen de watersector wordt goed samengewerkt (zie BAW) en is er een duidelijk gedeelde doelstelling: iedereen heeft belang bij een hoogstaande informatievoorziening. Bovendien is de BIO een gedeeld kader voor alle publieke partijen binnen de keten.

Voor andere informatie dan waterstanden, bijvoorbeeld bijzondere persoonsgegevens die het waterschap heeft (denk aan strafrechtelijke gegevens bij de afdeling toezicht en handhaving van een waterschap) is de kans op juridische knelpunten groter omdat daar verschillende wetsfamilies eisen stellen aan de informatieveiligheid.

1.2 Personae II Medewerker jeugdzorg

Monique werkt als medewerker bij een GGZ-instelling (een stichting). Monique verleent jeugdhulp (in de zin van de Jeugdwet) aan een jongen van 16 met ernstige psychische problemen, waaronder een drugsverslaving en een behoorlijk strafblad. Op een avond wordt Monique door de jongen geappt dat hij al twee weken onder een brug slaapt. Ze probeert meteen een plaats in een opvang te regelen en meldt de situatie in de verwijsindex risicojongeren. Deze melding blijkt niet de enige melding te zijn. Ook de politie heeft recent een melding geplaatst in de verwijsindex. Het systeem geeft aan dat er een match is en zowel de melder vanuit de politie als Monique krijgen een e-mail. Monique neemt meteen contact op met de politie en wisselt informatie over deze jongere uit en bepaalt op basis daarvan dat acute hulp noodzakelijk is.

BESCHRIJVING VAN HET REGELGEVEND KADER

In juridische zin verricht Monique jeugdhulp zoals dat omschreven staat in de Jeugdwet. Deze taken verricht Monique namens het college van de gemeente. Als uitvoerende professional moet Monique voldoen aan de kwaliteitseisen die de Jeugdwet stelt aan jeugdhulpaanbieders. Sommige van deze kwaliteitseisen zien op informatiebeveiliging. Verder gaat het in deze casus bijna uitsluitend om bijzondere persoonsgegevens en zijn naast de sectorale regelgeving, de regels over de bescherming en het gebruik van persoonsgegevens van toepassing (AVG, basisregistratie personen).

Juridisch gezien is er in deze casus sprake van twee moment van informatie-uitwisseling. De eerste is de informatie-uitwisseling binnen de verwijsindex risicojongeren. Deze verwijsindex bevat geen inhoudelijke informatie over de jongeren. Het bevat een identificatie van de jongere, identificatiegegevens van de meldende instantie, datum van de melding en contactgegevens van de melder.

Het tweede moment van informatie-uitwisseling ontstaat nadat er een “match” is. Dit leidt ertoe dat twee melders met elkaar in contact worden gebracht. Pas dan vindt inhoudelijke informatie-uitwisseling plaats. Deze inhoudelijke informatie-uitwisseling is vanuit juridisch perspectief een stuk ingewikkelder omdat zowel Monique als de politie de eigen sectorale informatieveiligheidseisen moeten hanteren.

Om gebruik te mogen maken van de verwijsindex moet Monique zorgdragen “voor een zorgvuldig en veilig gebruik van de verwijsindex”. Als Monique voldoet aan de eisen uit NEN 7510, wordt ze vermoed zorgvuldig en veilig de verwijsindex te gebruiken (zie Besluit Jeugdwet). Verder moet, op grond van het Besluit Jeugdwet, de aansluiting van de GGZ-instelling op de verwijsindex voldoen aan NTA 8023 (of een vergelijkbare norm). In het regelgevend kwadrant (zie hoofdstuk 2) is daarom sprake van een open norm gecombineerd met een verwijzing naar een standard.

Om in aanmerking te komen voor de politiegegevens op basis waarvan de politie een melding heeft gedaan, moet (de werkgever van) Monique voldoen aan de informatieveiligheidseisen uit de Wet politiegegevens en onderliggende regelgeving. In artikel 4:2, eerste lid, onderdeel i, van het

Besluit politiegegevens, staat een grondslag op basis waarvan de politie informatie over jeugdige aan Monique kan verstrekken. Daarbij is wel van belang dat het college, namens we ze jeugdhulp levert, daartoe rechten en bevoegdheden heeft toegekend. Mocht dat geregeld zijn geldt bij deze verstrekking een belangrijke informatiebeveiligingseis: de geheimhoudingsplicht uit artikel 7, tweede lid, van de Wet politiegegevens. Deze geheimhoudingsplicht luidt:

> *De persoon aan wie politiegegevens zijn verstrekt is verplicht tot geheimhouding daarvan behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt.*

De geheimhoudingsplicht is ook een open norm, die niet verder wordt uitgewerkt. Verder gelden voor beide informatie-uitwisselingen de algemene informatieveiligheidsregels die volgen uit de regelgeving over de bescherming van persoonsgegevens. Dit vertaalt zich bijvoorbeeld naar zorgplichten rond de “passende beveiliging van persoonsgegevens” (AVG). Dit zijn ook open normen. Deze zijn binnen de GGZ-instelling vertaald naar interne regels over het veilig gebruik van het Elektronisch cliëntendossier (ECD). Verder speelt de NTA7516 norm (kaders voor e-mailen in de zorg) een belangrijke rol.

DE VERHOUDING TUSSEN HET REGELGEVEND KADER EN HET DAGELIJKS WERK VAN MONIQUE

Voor Monique is het cruciaal om snel op basis van beschikbare, integere en vertrouwelijke informatie te kunnen handelen om de jongere te helpen. Daarbij staat vooral de vraag centraal: mag ik over deze informatie beschikken? Is er een grondslag? Deze vragen zijn door de gemeente vooraf uitgezocht zodat de partijen die meldingen doen in de verwijsindex vervolgens ook onmiddellijk relevante informatie kunnen uitwisselen en snel kunnen handelen om een jongere te helpen.

Voor de informatieveiligheidseisen geldt dat Monique erop vertrouwt dat de ICT die ze gebruikt om gegevens te registeren en te versturen, voldoet aan de zorgplichten die staan geformuleerd in de AVG, het Besluit Jeugdwet en de Wet politiegegevens. Monique gebruikt diverse systemen om gegevens aan te delen: soms gaat dit via een portal, soms per mail in excel. Ze vertrouwt daarbij op de aanwijzingen van de dienst van de GGZ-instelling die de bestuurlijke informatievoorziening regelt. Monique moet regelmatig naar trainingen en awareness-sessies om te borgen dat ze op een juiste manier met informatie om blijft gaan.

MOGELIJKE JURIDISCHE KNELPUNTEN

De juridische puzzel om Monique in staat te stellen op een rechtmatige en veilige manier informatie uit te wisselen, wordt niet door Monique zelf gemaakt. Deze puzzel wordt gemaakt door haar werkgever, de GGZ-instelling, en het college van B&W, namens wie ze de jeugdhulp levert. Daarbij valt op dat er veel sprake is van open normen, al dan niet aangevuld met een standaard.

In achtergrondgesprekken met CISO's van zorginstellingen en gemeenten blijkt wel dat het maken van deze puzzel erg veel inspanningen vergt. Voor ieder nieuw initiatief waarin informatie uitgewisseld wordt, gelden andere grondslagen en daaraan gekoppeld, wisselend geformuleerde informatieveiligheidsregels. Bij ieder nieuw initiatief hopen zorginstellingen en gemeenten dat er geen juridische belemmeringen zijn om de informatie-uitwisseling uit te voeren. Dit ziet zowel op het niveau van de bevoegdheid tot uitwisseling, als op de technische haalbaarheid wanneer meerdere informatieveiligheidseisen worden gesteld.