Beleid

Bescherming van persoonsgegevens en Informatiebeveiliging

2022

Voorwoord

In de huidige bedrijfsvoering is elektronische informatievoorziening niet meer weg te denken. We werken bijvoorbeeld dagelijks met digitale cliënt- en medewerkerdossiers; gebruiken steeds meer ondersteunende technologie voor zowel cliënten (e-health) als medewerkers en ook internet of things (slimme apparaten) wordt steeds vaker ingezet.

De toepassing en het belang van elektronische informatievoorziening zal alleen maar toenemen. Daarmee kan echter ook de privacy in het geding komen en worden de risico's op schending van de vertrouwelijkheid, beschikbaarheid of integriteit van de informatie door menselijke of technische fouten en cybercriminaliteit groter. Voor een veilige en betrouwbare bedrijfsvoering is daarom een adequate informatiebeveiliging en bescherming van persoonsgegevens essentieel.

Met dit beleid geeft de Raad van Bestuur richting aan de wijze waarop binnen ons concern uitvoering wordt gegeven aan de bescherming van persoonsgegevens en informatiebeveiliging.

De Raad van Bestuur,

R. Stegehuis A.M. Notermans

Inhoudsopgave

1 Inleiding

In dit document geven we weer wat de centrale doelstellingen zijn voor Espria en haar onderdelen op het gebied van de bescherming van persoonsgegevens en informatiebeveiliging. Ook is beschreven hoe we de risico's op dat gebied willen beheersen en hoe we het organisatorisch hebben ingericht.

Dit beleid geeft een centraal kader voor het concern Espria. Groepsmaatschappijen formuleren op basis hiervan een eigen (aanvullende) uitwerking en kunnen daarin de onderwerpen (nader) benoemen die specifiek van belang zijn voor de eigen groepsmaatschappij.

De doelstellingen voor Bescherming van persoonsgegevens en Informatiebeveiliging komen voort uit:

- De behoefte van betrokkenen zoals cliënten en medewerkers dat hun persoonsgegevens adequaat beschermd worden en dat zij ten aanzien daarvan hun rechten kunnen uitoefenen;
- De behoefte van samenwerkingspartners en andere stakeholders om met een veilige en betrouwbare partij samen te werken/ afspraken te maken;
- De behoefte van Espria en haar groepsmaatschappijen om ten aanzien van informatiebeveiliging en bescherming van persoonsgegevens een veilige en betrouwbare organisatie te zijn.
- De eisen van Europese en nationale wet- en regelgeving;
- De eisen van relevante normen zoals die zijn vastgelegd in de meest actuele versies van de Norm voor Informatiebeveiliging in de zorg (NEN) of de meest actuele versies van andere relevante normen.

Het beleid is de eindverantwoordelijkheid van de raad van bestuur en wordt in de uitvoering doorgegeven aan de directies van de groepsmaatschappijen.

In dit document komen aan de orde:

- Juridisch kader
- Doelstellingen
- Beheersing
- Organisatie

De in dit beleid gebruikte terminologie is afkomstig van de Algemene Verordening Gegevensbescherming (AVG) en NEN7510. Voor een lijst van begrippen wordt verwezen naar artikel 4 AVG – Definities en Hoofdstuk 3 – Termen en Definities van de NEN7510-1:2017.

2 Juridisch kader

De basis voor dit beleid is de Europese en nationale wet- en regelgeving op het gebied van privacy, relevante normen (zoals NEN), jurisprudentie en besluiten van de AP. Hieronder is in het kort de meest relevante wet- en regelgeving beschreven. In **Bijlage 1** is een uitgebreidere beschrijving van relevante wet- en regelgeving opgenomen.

2.1 Bescherming van persoonsgegevens

De AVG beschermt de verwerking van persoonsgegevens van *natuurlijke* en *levende personen*.[1] Geregeld is in welke omstandigheden persoonsgegevens verwerkt mogen worden en wat de rechten van de betrokkenen zijn. De AVG legt verplichtingen op aan *verwerkingsverantwoordelijken*[2] en *verwerkers.*[3] Elke afzonderlijke groepsmaatschappij van Espria is aan te merken als een verwerkingsverantwoordelijke in de zin van de AVG en in bepaalde gevallen ook als verwerker.

Het concern Espria verwerkt dagelijks een aanzienlijke hoeveelheid persoonsgegevens, waaronder gegevens over de gezondheid. Gezondheidsgegevens zijn bijzondere persoonsgegevens in de zin van de AVG. Deze worden extra beschermd. Ook in andere wetten zijn regels opgenomen over de zorgvuldige omgang van gezondheidsgegevens, zoals in de WGBO.[4] Onder de WGBO hebben zorgverleners een medisch beroepsgeheim.[5] De AVG bestaat naast deze andere wetten en de regels voor het medisch beroepsgeheim.[6]

2.2 Informatiebeveiliging

AVG

Een verwerkingsverantwoordelijke is *in het algemeen* verplicht om passende[7] technische en organisatorische maatregelen te nemen *om te waarborgen en te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd*.[8] Van de verwerkingsverantwoordelijke wordt verwacht dat de genomen maatregelen worden uitgewerkt in een beleid dat in de praktijk wordt gebracht. De verwerkingsverantwoordelijke is *in het bijzonder* verplicht om technische en organisatorische maatregelen te treffen die passen bij het risico.[9] Er dient rekening te worden gehouden met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's voor de rechten en vrijheden van personen, de aard, de omvang, de context en de verwerkingsdoeleinden. Bij de beoordeling of er een passend beveiligingsniveau is, zal met name rekening moeten worden gehouden met de verwerkingsrisico's: vernietiging, verlies, wijziging, ongeoorloofde verstrekking of onge-

[1] Artikel 1.1 AVG. De AVG is niet van toepassing op persoonsgegevens van overleden personen, zie Overweging 27 AVG.
[2] Verwerkingsverantwoordelijke is '*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt*', artikel 4.7 AVG.
[3] Verwerker is 'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt'.
[4] Maar ook de Wkkgz, Wet BIG, Zvw, Wmg en Wabvpz.
[5] Het medisch beroepsgeheim van de Wet geneeskundige behandelingsovereenkomst (Wgbo) houdt niet op te bestaan als cliënten overlijden.
[6] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg
[7] De maatregelen moeten passen bij aard, omvang, context en doel van de verwerking en proportioneel zijn daarvoor, zie Artikelsgewijs commentaar AVG, Engelfriet e.a., editie 2018, artikel 24, p. 116.
[8] Artikel 24 AVG.
[9] Artikel 32 AVG. Geldt voor ook voor verwerkers.

oorloofde toegang). De AVG biedt de verwerkingsverantwoordelijke de mogelijkheid om het aansluiten bij een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme, zoals NEN, te gebruiken om aan te kunnen tonen dat verplichtingen en vereisten worden nageleefd

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en het Besluit Elektronische gegevensverwerking door zorgaanbieders (Wabvpz)
In de Wabvpz zijn onder meer regels opgenomen voor zorgaanbieders ten aanzien van elektronische verwerking van gegevens. In deze wet is ook aangegeven dat er nadere regels kunnen worden gesteld over 'de functionele, technische en organisatorische maatregelen voor het beheer, de beveiliging en het gebruik van een zorginformatiesysteem of een elektronisch uitwisselingssysteem'. Deze nadere regels zijn uitgewerkt in het Besluit Elektronische gegevensverwerking door zorgaanbieders.

Besluit Elektronische gegevensverwerking door zorgaanbieders
In het Besluit Elektronische gegevensverwerking door zorgaanbieders is vastgelegd dat zorgaanbieders in overeenstemming met het bepaalde in NEN7510 en NEN7512 dienen zorg te dragen voor een veilig en zorgvuldig gebruik van het *zorginformatiesysteem* en een veilig en zorgvuldig gebruik van het *elektronisch uitwisselingssysteem* waarop zij zijn aangesloten.[10] Een zorginformatiesysteem is gedefinieerd als een elektronisch systeem van een zorgaanbieder voor het verwerken van persoonsgegevens in een dossier[11], niet zijnde een elektronisch uitwisselingssysteem.[12] Een elektronisch uitwisselingssysteem is een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier.[13] In het Besluit is ook vastgelegd dat als een zorgaanbieder verantwoordelijk is voor een zorginformatiesysteem of voor een elektronisch uitwisselingssysteem, hij ervoor zorg dient te dragen dat de logging van het betreffende systeem voldoet aan het bepaalde in NEN 7513.[14]

NEN 7510
NEN 7510-1 voorziet in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en kan worden gebruikt om het vermogen van de organisatie te beoordelen om te voldoen aan de eigen informatiebeveiligingseisen. NEN 7510-2 geeft beheersmaatregelen voor het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonlijke gezondheidsinformatie.

NEN 7512
De NEN 7512 is een aanvulling op de beheersmaatregelen in NEN 7510 en heeft betrekking op de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, met zorgverzekeraars en andere partijen die bij de zorg zijn betrokken. De norm beschrijft 'het classificeren van de gegevensuitwisseling en het bepalen van het risico hiervan. Op basis van die classificatie worden voor de gegevensuitwisseling minimumeisen gesteld met betrekking tot de bron van de gegevens, het transportkanaal en de ontvanger van de gegevens'. [15]

NEN 7513

[10] Artikel 3, tweede lid Besluit Elektronische gegevensverwerking door zorgaanbieders.
[11] Een schriftelijk of elektronisch vastgelegde gegevens met betrekking tot de verlening van zorg aan een cliënt, artikel 1, onderdeel i Wabvpz.
[12] Artikel 1 Besluit Elektronische gegevensverwerking door zorgaanbieders.
[13] Artikel 1, onderdeel j Wabvpz.
[14] Artikel 5, eerste lid Besluit Elektronische gegevensverwerking door zorgaanbieders.
[15] NEN7512, hoofdstuk 1.

NEN 7513 is een nadere uitwerking van hetgeen in NEN 7510 is vermeld over logging. In NEN 7513 is beschreven welke gebeurtenissen moeten worden gelogd, welke gegevens van die gebeurtenissen moeten worden vastgelegd, aan welke kwaliteitseisen het loggen en de logbestanden moeten voldoen en hoe lang de logbestanden moeten worden bewaard.

NTA 7516
In de Nederlandse Technische Afspraak Veilig mailen (NTA) 7516 zijn randvoorwaarden gegeven voor een veilige en betrouwbare uitwisseling van persoonlijke gezondheidsinformatie via e-mail en chatapplicaties. De NTA 7516 is onder meer gebaseerd op de AVG en vormt een aanvulling op de normen die er al zijn voor het verwerken van persoonlijke gezondheidsinformatie, zoals NEN 7510. Het wettelijk kader dat geldt voor de NEN 7510, 7512 en 7513, geldt hier ook.

3 Doelstellingen

De algemene doelstellingen van (het concern) Espria zijn:

1. **Espria zorgt voor een adequate bescherming van persoonsgegevens (privacy). Dat betekent onder meer dat Espria ten aanzien van het verwerken van persoonsgegevens voor betrokkenen een veilige en betrouwbare organisatie is, dat betrokkenen hun rechten kunnen uitoefenen en dat Espria helder is over de wijze waarop wordt omgegaan met persoonsgegevens.**

Om aan de eerste doelstelling te kunnen voldoen, is aangesloten bij het Privacy Control Framework van Norea. Deze biedt ondersteuning bij de beoordeling of de beheersingsdoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden behaald. Dit Framework bevat beheersingsdoelstellingen waarmee vastgesteld kan worden of maatregelen ten aanzien van privacybescherming adequaat zijn om te voldoen aan (wijzigingen in) wetgevingskaders (zoals de AVG). In het Framework zijn in totaal 95 beheersingsmaatregelen opgenomen, verdeeld over 32 onderwerpen in 9 fasen van het levenscyclusmanagement. In onderstaande tabel zijn de fasen uit het levenscyclusmanagement en de onderwerpen weergegeven. Het totale framework is te raadplegen via https://www.norea.nl/download/?id=6041.

Fase levenscyclusmanagement		**Onderwerpen**
1.	Management	Privacybeleid
		Afbakening van rollen en verantwoordelijkheden
		Identificatie en classificatie van persoonsgegevens
		Risicomanagement
		Data protection impact assessments
		Beheer van privacyincidenten en inbreuken
		Competenties medewerkers
		Bewustwording en training medewerkers
		Juridische toets van wijzigingen in wet- en regelgeving en/of bedrijfsvereisten
2.	Informeren	Privacyverklaring
3.	Keuze en toestemming	Toestemmingsraamwerk
4.	Verzamelen	Minimale gegevensverwerking
5.	Gebruiken, opslaan en verwijderen	Doelbinding
		Privacyarchitectuur (Gegevensbescherming door ontwerp en door standaard-instellingen)
		Bewaren van gegevens
		Verwijdering, vernietiging en anonimiseren
		Gebruik en beperking
6.	Inzage en kwaliteit van gegevens	Verzoek tot inzage
		Verzoek tot rectificatie
		Verzoek tot wissen
		Verzoek tot overdracht
		Juistheid en volledigheid van gegevens
7.	Verstrekken	Verstrekking aan derden en registratie
		Overeenkomsten met derden
		Doorgifte van persoonsgegevens

8.	Gegevensbeveiliging	Programma informatiebeveiliging
		Identiteit en toegangsbeheer
		Veilige gegevensoverdracht
		Versleuteling en eindpuntbeveiliging
		Registreren van toegang
9.	Monitoren en handhaven	Beoordeling van compliance met privacywetgeving
		Periodiek monitoren van privacybeheersingsmaatregelen

2. Espria zorgt voor adequate informatiebeveiliging. Dat betekent dat de beschikbaarheid, integriteit en vertrouwelijkheid van persoonlijke (gezondheids)informatie beschermd wordt en dat de toegang tot dergelijke informatie gecontroleerd en verantwoord kan worden.

Om aan deze doelstelling te kunnen voldoen, is aangesloten bij NEN-normen. Hieronder is uitgewerkt in welke norm wat geregeld is en voor welke onderwerpen eisen en beheersmaatregelen zijn geformuleerd. De precieze eisen en beheersmaatregelen zijn in de betreffende normen zelf te raadplegen.

NEN 7510-1	**NEN 7510-2**	**NEN 7512**	**NEN 7513**
Eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging	**Beheersmaatregelen voor het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonlijke gezondheidsinformatie**	**Gegevensuitwisseling in de zorg** *Aanvulling op de beheersmaatregelen van NEN 7510*	**Logging** *Aanvulling op NEN 7510-2*
Context van de organisatie	Informatiebeveiligingsbeleid	Vertrouwensbasis voor gegevensuitwisseling	Informatiebehoeften
Leiderschap	Organiseren van informatiebeveiliging	Risicobeheersing van de gegevensuitwisseling	Te loggen gebeurtenissen
Planning	Veilig personeel	Beheersmaatregelen: - Te maken afspraken - Beleid en procedures - Uitwisselingsovereenkomsten - Beheer dienstverlening door derde partij - Bedieningsprocedures - Uitvoering van de afspraken - Toekenning en beheer identificatoren - Registratie van entiteiten - Authenticatie - Elektronische berichtenuitwisseling - Ondertekening - Logging - Beheer en naleving - Informatiebeveiligingsincidenten - Capaciteitsbeheer - Back up en herstel - Continuiteitsbeheer - Naleving	Gegevensvelden in de logging
Ondersteuning	Beheer van bedrijfsmiddelen		Zekerheidseisen
Uitvoering	Toegangsbeveiliging		Weergave van de logging
Evaluatie	Cryptografie		
Verbetering	Fysieke beveiliging en beveiliging van de omgeving		
	Beveiliging bedrijfsvoering		
	Communicatiebeveiliging		
	Acquisitie, ontwikkeling en onderhoud van informatiesystemen		
	Leveranciersrelaties		
	Beheer van informatiebeveiligingsincidenten		
	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer		
	Naleving		

4 Beheersing

4.1 ISMS/ GRC tool

Het beheersen van de bescherming van persoonsgegevens en informatiebeveiliging geschiedt aan de hand van een managementsysteem voor informatiebeveiliging (Information Security Management System; ISMS). Met een ISMS kan aan de hand van een systematische aanpak de beveiliging van informatie bestuurd worden. Espria heeft een GRC tool in gebruik genomen die voorziet in een dergelijke systematische aanpak. Deze tool bevat standaard de beheersmaatregelen van het Privacy Control Framework van Norea en de normen van NEN 7510. Deze worden gekoppeld met de processen en middelen van de Espria-onderdelen., waarmee goed inzichtelijk en aantoonbaar kan worden gemaakt hoe het per Espria-onderdeel gesteld is met de bescherming van persoonsgegevens en de informatiebeveiliging. Het is mogelijk om zelf andere normen toe te voegen en te koppelen.

4.2 PDCA

In de tool wordt conform de NEN 7510 gewerkt met een PDCA-cyclus. Deze cyclus bestaat uit de volgende fases:[16]

a) Plan: vaststellen
b) Do: implementeren en uitvoeren
c) Check: bewaken en beoordelen
d) Act: bijhouden en verbeteren

4.2.1 Vaststellen (plan)

Deze fase bestaat uit beleidsvorming, risicoanalyse en verbeterplannen.

- *Beleidsvorming:* in onderhavig beleid worden de doelstellingen voor bescherming van persoonsgegevens en informatiebeveiliging van Espria vastgelegd. De raad van bestuur stelt dit beleid vast. Hiermee vormt het beleid de basis.
- *Risicoanalyse:* in de tool zijn de onderwerpen uit het Privacy Control Framework en de NEN-normen opgenomen. Deze worden gekoppeld met middelen en processen van de Espria-onderdelen, zodat daar risicoanalyses op kunnen worden uitgevoerd. Elk Espria-onderdeel maakt zijn eigen analyses. In de risicoanalyse is een compliancy-toets aan wet- en regelgeving begrepen. Het analyseren van de risico's/ eventuele non-compliance heeft tot doel:
  1. Inzicht te krijgen op welke punten niet of niet geheel wordt voldaan aan wet- en regelgeving.
  2. Inzicht te krijgen in de kwaliteit en de effectiviteit van de bestaande beveiligingsmaatregelen.
  3. Inzicht te krijgen in de risico's die het gaan voldoen aan wet- en regelgeving of de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen.
  4. Het gewenste niveau van bescherming van persoonsgegevens en informatiebeveiliging vast te stellen met een classificatie van bedrijfsprocessen, informatiesystemen en gegevensverzamelingen.
  5. Keuzes te kunnen maken voor het verbeteren van compliancy of beheersen van risico's.
  6. Prioriteiten te bepalen ter verbetering van de bestaande situatie.
- *Verbeterplannen: o*p basis van de uitkomsten van de risicoanalyses worden een verbeterplannen opgesteld. De verbeterplannen worden in geval van algemene analyses vastgesteld door de Raad van Bestuur en bij de specifieke analyses aan de opdrachtgever van de risicoanalyses. In de tool worden de maatregelimplementaties en controles op maatregelen en implementaties ingepland.

[16] NEN7510-2:2017, p. 163.

4.2.2 Implementatie en uitvoeren (do)

Aan de hand van de verbeterplannen wordt de implementatie en uitvoering van maatregelen ter hand genomen. Via de tool worden maatregelen geïmplementeerd, incidenten opgelost, algemene taken uitgevoerd, documenten gereviewd en procesdoelstellingen, middeldoelstellingen en doelstellingen per organisatieonderdeel geaccordeerd. Deze taken worden vanuit de tool aan diverse medewerkers door gezet.

4.2.3 Bewaken en beoordelen (check)

Het niveau van de bescherming van persoonsgegevens en informatiebeveiliging binnen Espria wordt met de tool bewaakt. Enerzijds is er zicht op de risico's en de aanpak daarvan, anderzijds voorziet de tool in de volgende controlevormen:

- Maatregelcontroletaken: operationele controle op de naleving van het beleid en de hieruit voortvloeiende richtlijnen en maatregelen;
- Implementatiecontroletaken: controle op de voortgang van de implementatie en borging van het beleid en de hieruit voortvloeiende richtlijnen en maatregelen;
- Audittaken: onafhankelijke controle.

4.2.4 Bijhouden en verbeteren (act)

Op basis van de uitkomsten van evaluaties en controles of door nieuwe ontwikkelingen kan het nodig zijn om het beleid bij te stellen, nieuwe risicoanalyses (waaronder compliancytoetsen aan wet- en regelgeving) uit te voeren, extra maatregelen te treffen of de implementatie hiervan aan te passen. Verder kunnen ontwikkelingen, zoals nieuwe bedrijfsprocessen of informatiesystemen, aanleiding zijn om het beleid te heroverwegen. Via de tool worden verbeteracties uit maatregel- en implementatiecontroles en uit interne en externe audits uitgezet.

4.3 Rapporteren

De Liso's van de Espria-onderdelen rapporteren de voortgang van het beheersen van de bescherming van persoonsgegevens en informatiebeveiliging in de 4M, 8M en 12M rapportages. Deze rapportages zijn risicogebaseerd. In de tool is inzichtelijk welke middelen en/ processen (de meeste) risico's geven. De Liso's delen de rapportages met hun directies en zetten deze vervolgens door naar de FG. De FG stelt van de afzonderlijke M-rapportages een geconsolideerde Espria rapportage op. Deze Espria rapportage vormt onder meer input voor de gesprekken die tussen de raad van bestuur en de directies plaatsvinden.

4.4 Non-compliance

Hierboven is beschreven dat als bepaalde middelen of processen risicovol zijn, er verbetermaatregelen worden genomen. Als ten aanzien van deze verbetermaatregelen een deadline is gesteld, dan is er een mogelijkheid dat een Espria-onderdeel op deze datum nog niet (geheel) voldoet aan deze maatregelen. Het nog niet voldoen aan de maatregelen wordt door de directies van de Espria-onderdelen aan de hand van een '*comply or explain*'-procedure (zie **Bijlage 2**) aan de raad van bestuur en FG gerapporteerd. Hierin wordt beschreven wanneer wel en aan de hand van welke stappen aan de maatregelen wordt voldaan. Deze explains worden in de M4, M8 en M12-rapportages meegenomen.

4.5 Disciplinaire procedure

Bij niet naleving van het beleid kunnen er maatregelen genomen worden. Het treffen van maatregelen heeft primair een lerende functie. Een maatregel kan bijvoorbeeld bestaan uit een gesprek om de

bewustwording te vergroten. In bepaalde gevallen kunnen er echter redenen zijn om tot *disciplinaire* maatregelen over te gaan. Voor de *disciplinaire* procedure geldt dat:[17]

a) Deze pas wordt gestart als is geverifieerd dat er sprake is van een overtreding;
b) Deze waarborgt dat medewerkers die worden verdacht van een overtreding correct en eerlijk worden behandeld;
c) deze voorziet in een maatregel die zorgvuldig en proportioneel is, waarbij rekening wordt gehouden met in ieder geval de volgende factoren:
   - de aard en ernst van de overtreding;
   - de impact op de bedrijfsvoering;
   - een eerste of herhaalde overtreding;
   - al dan niet juist getrainde overtreder;
   - relevante wetgeving;
   - zakelijke contracten.

Bij opzettelijke overtredingen kan onmiddellijke actie vereist zijn. De verantwoordelijke directie of raad van bestuur kan bij overtreding van dit beleid tot disciplinaire maatregelen overgaan.

4.6 Externe deskundigheid

4.6.1 Technische informatiebeveiliging

Medio 2018 is een overeenkomst gesloten met Fox-IT. Deze organisatie levert een aantal diensten waarmee het niveau van technische informatiebeveiliging verhoogd kan worden. Espria neemt de volgende diensten van Fox-IT af:

Cyber Security Assessment
Aan de hand hiervan wordt vastgesteld in welke mate Espria de technische beveiliging op orde heeft.[18] Het assessment bestaat uit:

- Een bedrijfs-, risico- en maturity assessment (rapportage, inclusief concreet actieplan);
- Een architectuurreview (rapportage met een overzicht van potentiële kwetsbaarheden in de architectuur, inclusief verbetervoorstellen);
- Een penetratietest waarbij op verschillende manieren aanvallen worden uitgevoerd, inclusief social engineering, malware en phishing (rapportage met bevindingen en aanbevelingen).

Managed Security Monitoring
Hiermee wordt het netwerk continue gemonitord. Er worden twee sensoren in de Espria datacenters geplaatst. De data die deze sensoren genereren, worden 7 dagen per week en 24 uur per dag door Fox-IT bewaakt. Bij verdachte situaties neemt Fox-IT binnen 15 minuten contact op met Espria (’s nachts met de consignatiedienst).

Incident Response
Deze dienstverlening ziet op situaties waarbij zich een incident (bijvoorbeeld datalek) heeft voorgedaan en bestaat onder meer uit:

- Directe bereikbaarheid voor support ingeval van een incident;
- Ondersteuning (hands-on) bij de reactie op het incident en bij forensisch onderzoek;
- Opleiding van Espria-medewerkers in het omgaan met incidenten.

[17] Zie NEN7510-2: 2017, paragraaf 7.2.3
[18] Eind 2016 is er een penetratietest uitgevoerd en zijn naar aanleiding daarvan vele verbeteringen doorgevoerd.

4.6.2 Voldoen aan NEN-normen

Het SSC en ZCN hebben in 2019 besloten zich te laten certificeren voor de NEN7510. Het SSC is sinds september 2020 gecertificeerd tegen NEN 7510 en ISO 27001. Jaarlijks vindt er een opvolgaudit plaats. Bij ZCN is de certificering in 2021 gepauzeerd in verband met een fusietraject. .

Bij certificatie- en compliancetrajecten wordt in relatief korte tijd onder begeleiding van externe consultants veel eisen en beheersmaatregelen uit de NEN-normen op orde gebracht. Dit zijn intensieve trajecten, maar deze hebben wel als resultaat dat de betreffende onderdelen compliant zijn ten aanzien van de NEN 7510. Het Informatiebeveiligingsoverleg (IBO) wordt op de hoogte gehouden van de ontwikkelingen in deze trajecten.

5 Organisatie

5.1 Uitgangspunten

De uitgangspunten bij de organisatie van bescherming van persoonsgegevens en informatiebeveiliging zijn:

- De raad van bestuur is verantwoordelijk voor de naleving van gegevensbescherming en voor de informatiebeveiliging en bewaakt de voortgang van verbeteringen.
- De Local information security officer (Liso) van een groepsmaatschappij fungeert als voorbereider en bewaker van de uitvoering in opdracht van de directies van de groepsmaatschappijen.
- De voortgang wordt geborgd met plannen, mijlpalen en afspraken waarbij een realistische prognose gehanteerd wordt.
- Bestaande structuren (zoals lijnorganisatie, experttafels) zijn uitgangspunt. Voor specifieke taken worden aanvullende taakafspraken gemaakt en afgestemd met raad van bestuur.
- Het IBO wordt voorgezeten door de Raad van Bestuur (bij afwezigheid van de bestuurder zit de Functionaris voor Gegevensbescherming (FG) het IBO voor). In het IBO worden onderwerpen besproken die voor meerdere/ alle groepsmaatschappijen van belang zijn. Ook worden daar kwesties die de afzonderlijke groepsmaatschappijen overstijgen en/ of waar een gezamenlijke aanpak wenselijk is, besproken en gecoördineerd.
- De functionaris voor gegevensbescherming (FG) heeft een adviserende taak en houdt intern toezicht op het naleven van de AVG en andere relevante wet- en regelgeving. De FG is onafhankelijk bij de vervulling van de taken.[19] De FG stelt ten behoeve van het toezicht een auditcharter en een auditjaarplan op. De uitkomsten van de audits geven mede inzicht voor het jaarlijks vaststellen van prioriteiten. In dat programma is ook ruimte voor Liso's om onder coördinatie van de FG audits/ toetsen uit te voeren bij andere groepsmaatschappijen dan de eigen groepsmaatschappij.

5.2 Three lines of defence

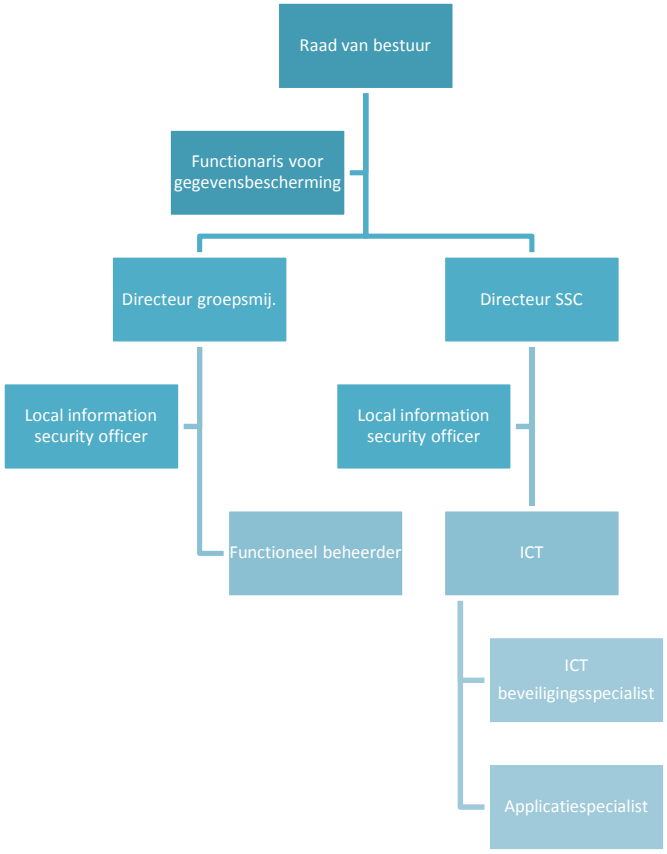
Bij de bescherming van persoonsgegevens en informatiebeveiliging wordt binnen Espria het *three lines of defence* model toegepast:

- *Eerste lijn:* het lijnmanagement (de eerste lijn) is verantwoordelijk voor de eigen processen.
- *Tweede lijn*: ondersteunt, adviseert, coördineert en bewaakt of het management deze verantwoordelijkheden ook daadwerkelijk neemt. Ook bepaalde beleidsvoorbereidende taken en het organiseren van integrale risk assessments zijn taken van de tweede lijn (Liso's, gezamenlijke taken, zie paragraaf 5.3).
- *Derde lijn*: controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en geeft daarover een objectief, onafhankelijk oordeel met mogelijkheden tot verbetering. Deze derde lijn opereert onafhankelijk van alle andere organisatieonderdelen (FG).

[19] Richtlijnen voor functionarissen voor de gegevensbescherming, WP29, 5 april 2017, paragraaf 3.3.

5.3 De functies

De meest betrokken functies zijn samengevat in onderstaande figuur.



5.3.1 Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming (FG) is een onafhankelijk intern toezichthouder van wie de functie is beschreven in de artikelen 36 tot en met 39 van de AVG. De FG houdt toezicht op en geeft advies aan de RvB over de verwerking van persoonsgegevens en informatiebeveiliging. De FG kan operationeel/tactische taken bij de decentrale Liso's beleggen.

De taken van de FG zijn onder meer:

- Informeert en adviseert de raad van bestuur over verplichtingen uit hoofde van de AVG en andere wet- en regelgeving op het gebied van bescherming van persoonsgegevens en informatiebeveiliging.
- Ziet toe op de naleving van de AVG en andere wet- en regelgeving op het gebied van bescherming van persoonsgegevens en informatiebeveiliging.
- Stelt concernbre(e)d(e) beleid, richtlijnen, kaders en modellen op ten aanzien van de bescherming van persoonsgegevens en informatiebeveiliging.
- Verzamelt informatie om verwerkingsactiviteiten te identificeren,
- Analyseert en controleert de naleving van verwerkingsactiviteiten,
- Informeert, adviseert een doet aanbevelingen aan verwerkingsverantwoordelijken of verwerkers.
- Stelt een auditcharter en een auditjaarplan op.

- Adviseert, informeert en doet aanbevelingen aan de Espria-onderdelen over verwerking van persoonsgegevens en informatiebeveiliging.
- Adviseert gevraagd en ongevraagd over uitvoering van beleid op het gebied van bescherming van persoonsgegevens en informatiebeveiliging en inzet van ondersteunende middelen.
- Ziet toe op de uitvoering en toepassing van beleid op het gebied van bescherming van persoonsgegevens en informatiebeveiliging;
- Adviseert gevraagd en ongevraagd over richtlijnen/ beleid voor verschillende privacy-onderwerpen, zoals registers van verwerkingen, verwerkersovereenkomsten, rechten van betrokkenen, DPIA's, en dergelijke ;
- Zorgt voor afstemming van beleid en -richtlijnen over de Espria-onderdelen heen en rapporteert over voortgang.
- Adviseert Espria-onderdelen t.a.v. het uitvoeren van Data Protection Impact Assessments (DPIA's).
- Ziet toe op de uitvoering van DPIA's op informatiesystemen en –projecten op Espria-niveau.
- Ziet toe op het (intern) melden en documenteren van mogelijke datalekken;
- Stelt KPI's op voor het proces datalekmanagement en rapporteert hierover;
- Voert audits uit en rapporteert hierover aan de raad van bestuur;
- Stelt geconsolideerde rapportages op (4M, 8M en 12M) en rapporteert hierover aan de raad van bestuur;
- Werkt samen met de AP;
- Treedt op als aanspreekpunt voor de Autoriteit Persoonsgegevens zoals voorafgaand overleg bij verwerkingen met hoog risico, geven van nadere informatie bij een datalek of klachten over de gegevensverwerking van Espria die de Autoriteit Persoonsgegevens bereiken. Indien contact met de Autoriteit Persoonsgegevens noodzakelijk is, wordt dit vooraf voorgelegd aan de raad van bestuur.
- Houdt zich actief op de hoogte van wet- en regelgeving, normenkaders en ontwikkelingen binnen het domein en anticipeert hierop.
- Coördineert en neemt deel aan het informatiebeveiligingsoverleg (IBO).

5.3.2 Local information security officer

De Local information security officer (Liso) heeft een positie binnen een Espria onderdeel en rapporteert aan de directie van dat onderdeel. Hij werkt vanuit kaders die op concernniveau worden vastgesteld en is betrokken bij het onderhoud van die kaders, maar richt zich vooral op de naleving daarvan in de operationele processen. De Liso heeft een toegevoegde waarde door zijn kennis van het bedrijfsonderdeel en de vertaalslag die moet worden gemaakt van algemene normen voor bescherming van persoonsgegeven en informatiebeveiligingsnormen naar de specifieke bedrijfssituatie. De Liso is verantwoordelijk voor de uitvoering van het ISMS (Information Security Management System) op decentraal niveau. Hij is het aanspreekpunt voor het lijnmanagement en is verantwoordelijk voor implementatie van het beleid ten aanzien van bescherming persoonsgegevens en informatiebeveiliging, dat specifiek is voor het bedrijfsonderdeel.

De taken van de Liso zijn onder meer:

- Stelt in samenspraak met de directie het organisatie specifiek jaarplan Bescherming persoonsgegevens en Informatiebeveiliging op, mede op basis van het concernbeleid Bescherming Persoonsgegevens en Informatiebeveiliging en de in het IBO vastgestelde speerpunten, draagt bij aan de implementatie hiervan en bewaakt de naleving van gemaakte afspraken.
- Adviseert en ondersteunt de directie en management en andere medewerkers binnen het organisatieonderdeel rondom informatiebeveiliging en bescherming persoonsgegevens.
- Adviseert over informatiebeveiliging en de bescherming van persoonsgegevens bij projecten en wijzigingen.

- Toetst interne werkwijzen aan de wet en regelgeving en normenkaders op het gebied van bescherming persoonsgegevens en informatiebeveiliging.
- Verzorgt en coördineert trainingen rondom informatiebeveiliging en bescherming persoonsgegevens voor directie, management en medewerkers op alle niveaus.
- Verzorgt communicatie en voorlichting rondom informatiebeveiliging en bescherming persoonsgegevens.
- Stimuleert bewustzijn binnen de organisatie o.a. door het opstellen, implementeren en onderhouden van een bewustwordingsprogramma.
- Draagt zorg voor inrichting en het beheer van het information security managementsysteem;
- Registreert incidenten, handelt incidenten (waar nodig in afstemming met de FG) af en adviseert met het oog op preventie.
- Monitort en rapporteert risico's.
- Bewaakt relevante aspecten van ontwikkeltrajecten.
- Signaleert trends en onderneemt hierop adequate acties.
- Toetst in afstemming met de FG periodiek de informatiebeveiligingsmaatregelen en de maatregelen ter bescherming van persoonsgegevens die binnen de organisatie zijn geïmplementeerd, o.a. door het realiseren van assessments, tests, reviews en audits en rapporteert aan de directie over de maatregelen, de activiteiten en de resultaten daarvan.
- Stelt waar nodig DPIA's op.
- Realiseert risicoanalyses en monitort en rapporteert over risico's aan eigen directie, het IBO (informatiebeveiligingsoverleg op Espria niveau) en Raad van Bestuur
- Beheert verwerkersovereenkomsten en houdt het verwerkingsregister bij.
- Indien directie de advisering omtrent omvangrijke risico's niet of niet tijdig opvolgt is er de mogelijkheid om te escaleren naar de FG. Deze situatie kan alleen ontstaan indien directie hiervan op de hoogte is.
- Treedt op als het eerste aanspreekpunt op het domein en wordt voor advies geconsulteerd door anderen.
- Acteert adequaat binnen crisissituaties, stelt onderzoek in, schakelt met belanghebbenden zodat er tot snelle besluitvorming gekomen kan worden. Initieert en neemt deel aan de verschillende commissies en stuur-, werk-, of projectgroepen binnen en buiten Icare
- Is verantwoordelijk voor het melden van datalekken bij de Autoriteit Persoonsgegevens , eventueel in afstemming met de FG;
- Is verantwoordelijk voor het onderhouden van contacten op het eigen domein. Is proactief teamlid, participeert in in- en externe samenwerkingsverbanden en onderhoudt relevante relaties
- Houdt zich actief op de hoogte van wet- en regelgeving, normenkaders en ontwikkelingen binnen het domein en anticipeert hierop.
- Neemt deel aan het Informatiebeveiligingsoverleg (IBO).

De Liso binnen het SSC heeft een aantal extra taken namelijk:

- Het vertalen van adviezen van de ICT-beveiligingsspecialist naar voorstellen voor aanpassingen van het IB-beleid;
- Het vertalen van het IB-beleid naar voorstellen voor ICT-beveiligingsrichtlijnen;
- Het implementeren van vastgestelde ICT-beveiligingsrichtlijnen voor de organisatie;
- In samenwerking met de ICT beveiligingsspecialist:
    - Het coördineren en afstemmen van de activiteiten bij onderzoek naar een ICT gerelateerd datalek;
    - Het initiëren en uitvoeren van ICT-beveiligingsprojecten;
    - Het initiëren en begeleiden van ICT-beveiligingsassessments, -tests, -reviews;
- Het functioneel aansturen van de ICT-beveiligingsspecialist.

5.3.3 ICT-beveiligingsspecialist

De taken van de ICT-beveiligingsspecialist zijn onder meer:

- Stelt verbetervoorstellen op voor het beveiligen van de ICT;
- Ontwerpt technische ICT-beveiligingsoplossingen;
- Realiseert technische beveiligingsmaatregelen en beveiligingsupdates in systemen en netwerken;
- Selecteert en implementeert beveiligingshulpmiddelen;
- Realiseert en monitort ICT-beveiligingsassessments, -tests en –reviews;
- Draagt bij aan forensisch onderzoek;
- Monitort en borgt de technische beveiligingsmaatregelen voor de ICT en evalueert ICT-beveiligingsrisico's;
- Presenteert verbetervoorstellen aan het lijnmanagement met betrekking tot ICT-beveiliging en -risico's.

5.3.4 Andere disciplines

Andere disciplines die betrokken zijn bij bescherming van persoonsgegevens en informatiebeveiliging zijn in **Bijlage 3** op een rij gezet.

5.4 Gezamenlijke taken

Onderstaande taken zijn gedeelde verantwoordelijkheden van de IBO-leden. Deze taken worden in afstemming met de CFO en in samenwerking tussen FG en Liso's uitgevoerd. In het IBO vindt daar afstemming over plaats. Het betreft het:

- Adviseren ter zake van een centrale (Espria brede) strategie voor privacybescherming en informatiebeveiliging voor de organisatie met veel ruimte voor strategie voor privacybescherming en informatiebeveiliging in de groepsmaatschappijen.
- Organiseren van samenhang tussen de activiteiten van de groepsmaatschappijen voor privacybescherming en informatiebeveiliging en de daarvoor benodigde expertise.
- Zorgen voor afstemming tussen privacybescherming en informatiebeveiliging met andere beveiligingsdomeinen, waaronder fysieke beveiliging en continuïteitsmanagement.
- Opzetten en onderhouden van een calamiteitenorganisatie op het gebied van bescherming van persoonsgegevens en informatiebeveiliging.
- Coördineren van de reactie op ernstige informatiebeveiligings- of ICT-incidenten.
- Zorgen voor een projectportfolio voor de uitvoering van de centrale strategie voor privacybescherming en informatiebeveiliging.
- Initiëren en coördineren van activiteiten en -projecten die nodig zijn ter uitvoering van de centrale strategie voor privacybescherming en informatiebeveiliging.
- Zorgen voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor privacybescherming en informatiebeveiliging. De principes van Privacy by design[20] en Privacy by default[21] zijn daarbij leidraad.
- Monitoren van de voortgang van realisatie en de kwaliteit van informatierisicoanalyses, privacy- en beveiligingsontwerpen en -oplossingen.
- Monitoren van het naleven van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Privacy by design en Privacy by default.

[20] Bij het ontwerpen van producten en diensten wordt ervoor zorggedragen dat persoonsgegevens goed worden beschermd. Daarbij worden niet meer gegevens verzameld dan noodzakelijk is voor het doel van de verwerking en worden de gegevens niet langer bewaard dan nodig is.

[21] Er worden technische en organisatorische maatregelen genomen om ervoor te zorgen dat standaard alléén persoonsgegevens verwerkt worden die noodzakelijk zijn voor het specifieke doel dat men wilt bereiken.

- Monitoren van het bewustzijn van informatiebeveiliging en privacy in de dagelijkse praktijk binnen de organisatie.
- Monitoren van de relevante risico's voor de organisatie.
- Borgen dat de organisatie voldoende voorbereid is op toekomstige privacy – en informatiebeveiligingsrisico's en ICT-beveiligingsrisico's.
- Monitoren van de kwaliteit van informatiebeveiligingsassessments, -tests, -reviews en -audits.
- Monitoren op basis van assessments, test, reviews en audits in hoeverre de organisatie compliant is met het informatiebeveiligingsbeleid en wet- en regelgeving.
- Informeren van algemeen management over de status van informatiebeveiliging en incidenten en presenteren van verbetervoorstellen.
- Beoordelen jaarplannen en rapportages van groepsmaatschappijen.

5.5 Overlegvormen

5.5.1 Het IBO

Het IBO is een overleg van inhoudelijk deskundigen, de Liso's en de FG, voorgezeten door de Raad van Bestuur. Het IBO vergadert maandelijks. Zie **Bijlage 4** voor de samenstelling van het IBO.

Het overleg heeft de volgende taken:

- Ziet toe op de efficiënte en effectieve samenwerking en taakverdeling tussen de groepsmaatschappijen en ondersteunende disciplines als ICT, M&A, concernjurist, concernaudit et cetera,
- Ziet toe op de samenhang van projecten die nodig zijn voor het bereiken van specifieke beveiligingsresultaten,
- Stelt in het kader daarvan werkwijzen, uitgangspunten vast voor taken of momenten van beschikbaarheid van deelresultaten,
- Uitwisselen van ervaring, delen van voorbeelden,
- Adviseren over gezamenlijke onderwerpen in verband met deskundigheid en werkbesparing,
- Verdelen van taken bij uitzoeken van onderwerpen,
- Opbouwen van inzicht welke activiteiten nodig zijn en welke groepsmaatschappij daarvoor verantwoordelijk is voor specifieke beveiligingsresultaten,
- Samenwerken bij audits.

5.5.2 Werkgroepen IBO

Vanuit het IBO worden ten aanzien van specifieke onderwerpen werkgroepen gevormd. Op deze manier kan er een verdieping op het betreffende onderwerp plaatsvinden en kan het IBO daar goed over geadviseerd worden.

5.5.3 Themabijeenkomsten

Minimaal 4 keer per jaar wordt er voor de leden van het IBO een themabijeenkomst georganiseerd. De organisatie is in handen van steeds een ander groepje leden van het IBO. Het doel is om met alle leden van het IBO wat dieper op een bepaald onderwerp in te gaan en deze met elkaar te bespreken.

5.5.4 Coördinatiegroepen Espria-onderdelen

De Liso's organiseren binnen het eigen onderdeel een coördinatiegroep bestaande uit een lid van de directie en het meest betrokken management. Deze groep draagt zorg voor:

- Inzicht opbouwen en onderhouden van de feitelijke situatie rond informatiebeveiliging binnen de eigen groepsmaatschappij en voldoen aan de privacywetgeving,
- Beoordelen van risico's, treffen van maatregelen om die risico's te bestrijden op het niveau van de groepsmaatschappij of naar aanleiding van incidenten,
- Opstellen van een plan van activiteiten voor bescherming van persoonsgegevens en informatiebeveiliging (activiteit, resultaat, budget, tijdspad),

- Uitvoeren van dat plan en van plannen die op advies van het IBO zijn geformuleerd,
- Rapporteren aan de directie van de groepsmaatschappij en het IBO over de voortgang.

De vergaderingen vinden met regelmaat plaats. Daarvan worden bij voorkeur notulen en actielijsten opgemaakt. De Liso stelt plannen op inclusief budgetten, bewaakt de voortang, signaleert waar nodig knelpunten.

5.6 Interne afbakening

5.6.1 Informatievoorziening

Ten behoeve van de Informatievoorziening is een Experttafel informatievoorziening (Experttafel IV) ingericht. Deze experttafel richt zich op de uitwisseling, opslag en bewerking van gegevens, inclusief de benodigde infrastructuur. In onderstaande tabel is het onderscheid tussen het IBO en de Experttafel IV weergegeven.

IBO	*Experttafel IV*
Focus op bescherming van persoonsgegevens en informatiebeveiliging	Focus op informatietechnologie: IV beleid, ICT en technologische innovatie
Voert regie over het beleid ten aanzien van het onderhouden van de bescherming van persoonsgegevens en informatiebeveiliging	Voert regie over de uitvoering van gezamenlijk IV-ICT beleid en alle gezamenlijke IV-ICT projecten (portfolio)
Ziet op voldoen aan relevante privacy wet- en regelgeving en beveiligingsnormen	Houdt relevante privacy wet- en regelgeving en beveiligingsnormen in acht
Ziet op borging van de vertrouwelijkheid, integriteit, beschikbaarheid van verwerkingen	Prioriteert op basis van belang, impact en urgentie.
Neemt passende maatregelen (modellen, werkwijzen, afspraken) om te faciliteren dat verwerkingen in overeenstemming met de AVG en veilig worden uitgevoerd.	Creëert samenhang en synergie (in IV- ICT projecten)

5.6.2 Financieel beheer

De administratieve organisatie en interne controle (AO/IC) borgt de juistheid, betrouwbaarheid, inzichtelijkheid en volledigheid van de administratie. Aan de hand van de goede werking van de AO/IC kan op adequate wijze financiële verantwoording worden afgelegd aan bijvoorbeeld verzekeraars of in het kader van de jaarrekening. In deze processen kunnen persoonsgegevens verwerkt worden. De rechtmatigheid, juistheid, inzichtelijkheid en volledigheid van het *financieel beheer* valt echter buiten het aandachtsgebied van dit beleid.

5.6.3 Kwaliteit

Hoe met (beveiliging van) persoonsgegevens wordt omgegaan, bepaalt mede (het ervaren van) de kwaliteit van zorg en bedrijfsvoering. Aspecten van informatiebeveiliging en bescherming van persoonsgegevens kunnen derhalve onderdeel zijn of worden van kwaliteitsmonitoren of kwaliteitscertificeringen, zoals HKZ.

5.6.4 E-health

De IGJ heeft een Toetsingskader “Inzet van e-health door zorgaanbieders” opgesteld. Dit kader geldt vanaf september 2018. Onder e-health verstaat de IGJ de inzet van hedendaagse informatie- en communicatietechnologie om de zorg te ondersteunen of te verbeteren. Bij e-health toepassingen kan gedacht worden aan beeldbellen, online inzage in het cliëntdossier of het gebruik van domotica. Het toetsingskader bestaat uit vijf thema’s, waarbij per thema een aantal normen is beschreven:

1. *Goed bestuur*: a. visie en beleid, b. organisatie, taken en verantwoordelijkheden, c. besluitvorming, d. Risicomanagement en e. controle over kosten, voortgang en kwaliteit.

2. *Invoering gebruik van e-health producten- en diensten*: a. aanschafprocedure, b. programma van eisen, c. risicoanalyse, d. training, e. testen en f. onderhoud.
3. *Patiëntparticipatie*: a. betrokken bij keuzes, b. goede informatie, c. afwegen geschiktheid, d. goede ondersteuning.
4. *Samenwerken in het netwerk en elektronisch vastleggen en uitwisselen van gegevens*: a. gegevensuitwisseling, b. medicatieoverdracht en c. overeenkomsten.
5. *Informatiebeveiliging en continuïteit*: a. managementsysteem voor informatiebeveiliging en b. continuïteit geborgd.

De thema's 4 en 5 bevatten onderwerpen die op het gebied van bescherming van persoonsgegevens en informatiebeveiliging liggen.

5.6.5 Integrated reporting

Espria werkt met een integrale rapportage van kwaliteit & veiligheid, financiën, mens & arbeid, internal audit en bescherming van persoonsgegevens & informatiebeveiliging. Elk deelgebied stelt een eigen jaarplan en charter op. De resultaten, kansen en risico's van de deelgebieden worden vervolgens in een geïntegreerde rapportage beschreven. Hiermee kan meer inzicht in de relatie tussen de deelgebieden worden gerealiseerd en kan geïntegreerd worden gestuurd op strategische doelen.

Bijlagen

1. Relevante wet- en regelgeving
2. Comply or explain procedure
3. Betrokken disciplines
4. Samenstelling IBO

Bijlage 1 Toepasselijke wet- en regelgeving

De volgende regelgeving is van toepassing voor bescherming van persoonsgegevens en informatiebeveiliging:

Algemene Verordening Gegevensbescherming (AVG)
De Algemene verordening gegevensbescherming (AVG) is van toepassing met ingang van 25 mei 2018 waarbij de Wet bescherming persoonsgegevens (Wbp) is vervallen. Een Verordening van de Europese Unie heeft directe werking voor de lidstaten waardoor de regels meer uniform zijn geworden. De vervallen Wbp was nog Nederlandse wetgeving die alleen richtlijnen van de Europese Unie moest volgen.

De AVG kent:

d) Tal van administratieve en organisatorische verplichtingen voor 'verwerkingsverantwoordelijken' zoals verantwoordingsplicht over de informatiebeveiliging, een register van de verwerkingsactiviteiten, verplichting voor grotere zorginstellingen om een FG aan te stellen, de verplichting om schriftelijke afspraken te maken met verwerkingsverantwoordelijken waarmee Espria samenwerkt of verwerkers die ten behoeve van Espria gegevens verwerken,
e) Rechten van betrokkenen zoals recht op vergetelheid of recht op beperken van de verwerking,
f) Versterkte bevoegdheden van de Autoriteit Persoonsgegevens waaronder de bevoegdheden om hoge bevoegdheden op te leggen.

De AVG bestaat naast bestaande wet- en regelgeving in de zorg.

Uitvoeringswet Algemene verordening gegevensbescherming
Bij het van toepassing worden van de AVG moesten nog een aansluiting worden gemaakt met de Nederlandse praktijk zoals de bekostiging van de Autoriteit Persoonsgegevens en regels hoe geschillen voor de rechter moeten worden gebracht. De Uitvoeringswet geeft op bepaalde onderdelen uitleg van de AVG.

Wet op de geneeskundige behandelingsovereenkomst (Wgbo)
De Wet op de geneeskundige behandelingsovereenkomst (Wgbo) maakt onderdeel uit van Boek 7 BW met de titel 'Bijzondere overeenkomsten'. In de Wgbo worden bijzondere regels gesteld voor geneeskundige handelingen waaronder verpleging en verzorging. Onder meer heeft de behandelaar een dossierplicht (7:454 BW) en een geheimhoudingsplicht (7:457 BW) binnen de overeenkomst.

Wet beroepen in de individuele gezondheidszorg (Wet BIG)
Deze wet regelt wettelijk beschermde beroepstitels voor de gezondheidszorg. Voor zover hier relevant zijn personen die werkzaam zijn in die titels tot geheimhouding verplicht [22] en zijn die personen ook onderworpen aan tuchtrechtspraak.

Wet aanvullende bepaling verwerking persoonsgegevens in de zorg (Wabvpz)
Bij de unanieme verwerping van het landelijke EPD in 2011, verzocht de Eerste Kamer om wetgeving die regels stelde voor de steeds grotere en talrijker regionale gegevensuitwisselingen in de zorg. Dit resulteerde in de wet Cliëntenrechtenzorg, een verzameling van uiteenlopende regelingen. Met eén

[22] Artikel 88 BIG: Een ieder is verplicht geheimhouding in acht te nemen ten opzichte van al datgene wat hem bij het uitoefenen van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of wat daarbij als geheim te zijner kennis is gekomen of wat daarbij te zijner kennis is gekomen en waarvan hij het vertrouwelijke karakter moest begrijpen.

daarvan werd de Wet Burgerservicenummer in de zorg (Wet BSN-z) aangevuld met art 15a tot en met 15i met gedetailleerde regels voor partijen die zorggegevens uitwisselen in een elektronisch uitwisselingssysteem en de verplichting om onderling afspraken te maken. De Wet BSN-z kreeg daarbij ook een andere naam: de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

De artikelen over computercriminaliteit in het wetboek van Strafrecht
Het gaat hier om een reeks van bepalingen om straf op te kunnen leggen voor bepaalde daden. Een voorbeeld is de strafbaarheid van 'computervredebreuk'[23] naar analogie van de al langer bestaande strafbaarheid van huisvredebreuk.

Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
De wet regelt de mogelijkheden voor patiënten om te klagen over zorgverleners (waaronder instellingen). Artikel 2 lid 1 van de wet luidt: "De zorgaanbieder biedt goede zorg aan." Algemeen aanvaard is dat dit een informatievoorziening impliceert zoals het dossier dat in de Wgbo verplicht is

Wet toelating zorginstellingen
Deze wet regelt dat de meeste zorginstellingen een toelating nodig hebben van de minister. De minister geeft die toelating alleen af als onder andere is voldaan aan eisen van 'ordelijke en controleerbare bedrijfsvoering', een eis die onder andere aandacht voor bescherming van persoonsgegevens en informatiebeveiliging impliceert.

Grondwet (artikel 10 en 13)
Artikel 10
- Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
- De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
- De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Artikel 13
- Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter.
- Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.

Eidas verordening
Vanaf 29 september 2018 is de Europese Eidas verordening van kracht. Publieke organisaties en private organisaties met een publieke taak moeten Europees erkende inlogmiddelen accepteren binnen de digitale dienstverlening. Deze verplichting geldt o.a. voor organisaties die gebruik maken van DigiD en eHerkenning[24].

---

[23] Artikel 138ab lid 1 Sr: Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel, of
d. door het aannemen van een valse hoedanigheid.

[24] https://www.digitaleoverheid.nl/dossiers/eidas/

Telecommunicatiewet
In art 11.7 van de Telecommunicatiewet is de Cookierichtlijn opgenomen. Daarin wordt gesteld dat iemand alleen gegevens mag opslaan op de randapparatuur van een gebruiker na informeren van de gebruiker en verkrijgen van toestemming. Een uitzondering is gemaakt voor opslag of toegang "die strikt noodzakelijk is om de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren of – mits dit geen of geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken abonnee of gebruiker – om informatie te verkrijgen over de kwaliteit of effectiviteit van een geleverde dienst van de informatiemaatschappij." (Art 11.7a lid 3 onder b – dit betreft het sessiooncookie dat nodig is voor de computer om te onthouden dat de gebruiker is ingelogd op een site).

Wet marktordening gezondheidszorg
De wet marktordening gezondheidszorg geeft belangrijke mogelijkheden aan de Zorgautoriteit en aan de zorgverzekeraars om kennis te nemen van zorggegevens. Belangrijk is dat het hier om wettelijke verplichtingen gaat waar de Zorgautoriteit of zorgverzekeraar een beroep op moet doen, de zorginstelling mag deze gegevens niet vrijwillig afgeven.

De Wet werk en inkomen naar arbeidsvermogen (WIA)
De WIA gaat onder andere in op arbeidsongeschiktheid, het voorkomen daarvan en re-integratie. De werknemer heeft verschillende verplichtingen om gegevens te verstrekken, de werkgever "houdt aantekening van het verloop van de ziekte en de re-integratie van de verzekerde" (art 41 lid 1).

Dit laatste is niet het bijhouden van een medisch dossier! De arbeidswetgeving kent andere uitgangspunten dan de zorg. In de zorg wordt aangenomen dat de cliënt in vrijheid kan beslissen over het delen van zorggegevens. In het arbeidsrecht wordt aangenomen dat de werknemer niet in vrijheid kan beslissen over het verstrekken van zorggegevens aan de werkgever omdat er sprake is van een afhankelijkheidsrelatie. Met andere woorden: de werknemer kan geen toestemming geven om zorggegevens te delen, de werkgever mag er ook niet om vragen. Zorggegevens zijn oor de AVG 'bijzondere gegevens' waarvan registratie verboden is behalve voor de in de AVG opgesomde instanties. De werkgever hoort daar niet bij.

De Wet Maatschappelijke ondersteuning 2015 en Jeugdwet
De gemeenten voeren deze wetten uit en kunnen daar zorginstellingen bij betrekken. Een voorbeeld is het toeleiden naar zorg, de beoordeling door een zorginstelling of iemand lettend op de criteria van de gemeente, recht heeft op een parkeervergunning. In dergelijke situaties gaat het om samenwerkingsverbanden tussen gemeenten en zorginstellingen. Deze Wetten geven de gemeenten ruime bevoegdheden om kennis te nemen van het zorgdossier waardoor het beroepsgeheim van de Wgbo niet kan worden ingeroepen.

Bijlage 2 Comply or explain procedure

Status: vastgesteld in het IBO van 13 december 2018

Inleiding

Het beleid Bescherming persoonsgegevens en Informatiebeveiliging (Beleid BPIB) beschrijft op hoofdlijnen de doelstellingen om ten aanzien van relevante wet- en regelgeving, waaronder AVG, WGBO en NEN-normen (NEN 7510, NEN7512 en NEN7513), compliant te zijn. Jaarlijks wordt in het IBO aan de hand van de doelstellingen een risico-inventarisatie gemaakt. Naar aanleiding van deze inventarisatie wordt een verbeterplan met maatregelen[25] opgesteld en uitgevoerd. Aan elk van de maatregelen van het verbeterplan moet op de daarvoor vastgestelde datum worden voldaan. De voortgang wordt gerapporteerd in de 4M, 8M en 12M. In de rapportages geven de groepsmaatschappijen zelf aan in hoeverre zij voldoen. Hierbij geldt het uitgangspunt: 'comply or explain'. Voor de maatregelen waarvoor de groepsmaatschappijen op de vastgestelde datum (nog) niet compliant zijn, vullen zij een Explain-formulier in.[26]

Wat is een Explain?

Een 'Explain' is een door de verantwoordelijk directeur[27] geaccepteerde verklaring waarom aan bepaalde maatregelen uit het verbeterplan niet (volledig) wordt voldaan.

In welke gevallen wordt een Explain-formulier ingevuld?

Een Explain-formulier moet worden ingevuld voor:

- Een maatregel waaraan op de daarvoor vastgestelde datum niet (volledig) voldaan wordt.
- Een maatregel waar een groepsmaatschappij om moverende redenen voor langere duur/ voor onbepaalde tijd niet aan zal voldoen. Een explain die hier op ziet, geldt voor een jaar, zodat er jaarlijks een nieuwe beoordeling plaats vindt.

Ter illustratie: voor 2018 is als maatregel benoemd dat met ingang van 31 december 2018 alle groepsaccounts opgeheven moeten zijn. Als een groepsmaatschappij op die datum nog niet alle groepsaccounts heeft opgeheven (of voor die datum al weet dat dat niet gaat lukken), dan vult de betreffende LISO een Explain-formulier in. Indien de groepsmaatschappij na afweging van belangen een gerechtvaardigde reden heeft om in een specifieke situatie voor een langere duur/ onbepaalde tijd een groepsaccount te blijven hanteren, dan wordt daarvoor ook een Explain-formulier ingevuld.

Veiligheid van systemen

Bij compliancy op het gebied van bescherming van persoonsgegevens en informatiebeveiliging hebben bedrijfskritische systemen prioriteit. Het gaat om systemen die bij falende beveiliging de bescherming van persoonsgegevens of de (kwaliteit van) dienstverlening in gevaar brengen. Ten aanzien van deze systemen wordt, bij het niet (volledig) voldoen, een Explain-formulier ingevuld.

Inhoud Explain

Een Explain-verklaring bevat onder meer:

- De maatregel of norm waaraan niet (volledig) wordt voldaan;
- De reden waarom nog niet kan worden voldaan of de reden waarom blijvend niet wordt voldaan;
- Het risico van het (nog) niet voldoen of blijvend niet voldoen:

---

[25] Acties die genomen moeten worden om de doelstellingen te halen.

[26] Voor deze notitie is gebruik gemaakt van de 'BIR comply or explainprocedure', d.d. 7 januari 2014, die deel uitmaakt van de Baseline Informatiebeveiliging Rijksdienst (BIR).

[27] Verantwoordelijk directeur: dit is de directeur die voor de uitvoering van het beleid verantwoordelijk is.

  - Voor betrokkenen;
  - Voor de eigen groepsmaatschappij;
  - Voor andere Espria groepsmaatschappijen;
  - Voor derden (andere organisaties);
- Reden van acceptatie van de Explain;
- Duur van het niet (volledig) voldoen;
- Naam van de verantwoordelijke groepsmaatschappij, de LISO (contactpersoon) en de verantwoordelijk directeur;
- De datum van de Explain;
- Status (kan tussentijds worden bijgehouden).

Procedure voor Explain binnen een groepsmaatschappij

Voor een explain die enkel ziet op één groepsmaatschappij, vult de LISO van de groepsmaatschappij de Explain in en legt deze voor aan de FG. De FG toetst de aanvraag onder meer met behulp van onderstaande vragen:

- Is de Explain inhoudelijk volledig ingevuld en onderbouwd?
- Zijn van de Explain de risico's duidelijk en is de tijdsduur bepaald (met verbeterplanning)?
- Zijn er risico's die invloed op andere groepsmaatschappijen hebben?
- Is de verwachting van de indiener dat een Explain binnen een half jaar verandert in een comply?

De FG voegt haar advies aan de aanvraag toe. Als het risico zich beperkt tot de groepsmaatschappij van de aanvrager, dan bepaalt de verantwoordelijke directeur of hij/ zij het advies van de FG overneemt en legt de beslissing in het Explain-formulier vast.

De LISO houdt de status van de explains bij en draagt er zorg voor dat explains met langere duur/ voor onbepaalde tijd na een jaar opnieuw gedaan en beoordeeld zullen worden.

Groepsmaatschappij overstijgende Explains

Als de risico's van het niet voldoen de groepsmaatschappij overstijgen, vult de LISO de Explain in en legt deze voor aan de FG. De FG toetst de aanvraag en voegt haar advies toe. De LISO legt de Explain vervolgens voor aan het IBO. Het IBO toetst de Explain onder meer aan de hand van:

- de risico's voor betrokkenen, andere groepsmaatschappijen of geheel Espria;
- de tijdsduur (met verbeterplanning);
- de verwachting dat een Explain binnen een half jaar verandert in een comply.

Het IBO weegt de risico's en komt tot een advies om de Explain goed of af te keuren. De verantwoordelijke bestuurder neemt een beslissing en deze wordt vastgelegd in de Explain, voorzien van het advies van de FG en het IBO.

Rapportage

In de 4M, 8M en 12M rapporteren de directies over actuele Explains.

Shared Service Center

Het SSC biedt diensten aan de groepsmaatschappijen en sluit daarvoor SLA's af. De groepsmaatschappijen zijn ten aanzien van deze diensten doorgaans de verwerkingsverantwoordelijke en daarmee ook verantwoordelijk voor het risicomanagement van deze diensten. Zij dienen inzichtelijk te maken hoe zij deze verantwoordelijkheid invullen. De groepsmaatschappijen maken in de SLA's afspraken met het SSC over het te leveren resultaat. Het SSC is verantwoordelijk voor het nakomen van deze afspraken (het resultaat) en moet aan de groepsmaatschappijen aantonen op dit punt in control te zijn.

EXPLAIN-FORMULIER **Beleid Bescherming persoonsgegevens en Informatiebeveiliging**	
Aanvrager	
Groepsmaatschappij	
LISO (contactpersoon)	
Datum aanvraag	
Beleid bescherming persoonsgegevens en informatiebeveiliging	
Beschrijving maatregel/ norm	
Verwerking/Proces/informatiesysteem	
Beschrijving verwerking/ proces/ informatiesysteem	
Doel verwerking/ proces/ informatiesysteem	
Afwijking van maatregel/ norm	
Beschrijving	
Reden/toelichting	
Risico's voor betrokkenen/ eigen groepsmaatschappij/ derden	
Risico voor andere groepsmaatschappijen van Espria?	
Oplossing/mitigerende maatregel	
Hoe lang blijft de afwijking bestaan?	
Advies FG	
Advies (goedkeuring Explain J/N)	
Toelichting	

Geldigheidsduur	
Toelichting	
Datum advies	
Advies IBO	
Advies (goedkeuring Explain J/N)	
Datum advies	
Toelichting	
Geldigheidsduur	
Besluit directeur (als het één groepsmij. betreft) *of* Besluit bestuurder (als het de afzonderlijke groepsmij. overstijgt)	
Naam verantwoordelijk directeur/ Naam bestuurder	
Goedkeuring Explain J/N	
Motivatie	
Datum ondertekening	
Handtekening	

Bijlage 3 Betrokken disciplines

Informatievoorziening en ICT - dragen zorg voor:

- Bepalen architectuur voor informatievoorziening en ICT
- Planning en realisatie van middelen die nodig zijn voor verbeteren van bescherming van persoonsgegevens en informatiebeveiliging bij de groepsmaatschappijen.

Juridische discipline - elke groepsmaatschappij is zelf verantwoordelijk voor het regelen van juridische discipline. De juridische discipline draagt zorg voor:

- Sjablonen voor contracten.
- Toets van contractvoorstellen: Espria-onderdelen leggen contracten ter beoordeling voor aan een jurist.

Websitebouw

- Formuleert eisen waaraan externe websites moeten voldoen.
- Toetst externe websites aan die eisen.

Communicatie – Centrale of decentrale communicatieadviseurs dragen zorg voor:

- Regelen beschikbaarheid van middelen voor bewustwording van medewerkers van het belang van informatiebeveiliging en de noodzaak van melden van datalekken,
- Definiëren van praktische instrumenten om te bepalen welk niveau van bewustwording is bereikt.

Inkoop – draagt zorg voor:

- Onderhoud contacten met leveranciers, ook voor het realiseren van nieuwe functionaliteiten die Espria nodig heeft om te voldoen aan de eisen van de AVG.
- Ontwerpt een strategie om juridisch effectief leveranciers medeverantwoordelijk te maken.

De groepsmaatschappijen zijn zelf verantwoordelijk voor de inhoudelijke afspraken. De FG geeft advies over het juridisch kader ten aanzien van de AVG en andere relevante privacy wet- en regelgeving.

Mens en Arbeid - draagt zorg voor:

- Implementeren van opleidingsprogramma's bij in dienst treden of tijdens in dienst zijn,
- Aanvullen van beoordelingsprocedures waar nodig ten aanzien van zorgvuldige omgang met informatie en informatiemiddelen.

Bijlage 4 IBO - Samenstelling

Overleg Bescherming Persoonsgegevens en Informatiebeveiliging ***Vergaderfrequentie: maandelijks***	
Liso De Trans	Daan van der Vlist
Liso Evean	Marcel Schaafsma
Liso Evean	Mariëlle de Groot
Liso GGZ Drenthe	Hans de Jong
Liso Icare	Anja Oosting
Liso JGZ	Isabel Benjamins
Liso ZG Meander	*vacature*
Liso ZCN	Bilal Hashmi
Liso Ledenvereniging	Bilal Hashmi
Liso SSC Espria	Erik Pieters
Functionaris voor gegevensbescherming	Marjolein van der Meij
Raad van Bestuur	Arthur Notermans