8 juli 2022 v1.3.2 definitief

Xadya van Bruxvoort, Victor Meerloo

Gemeente Arnhem

ONDERZOEK, ADVIES EN INRICHTING PRIVACY- EN INFORMATIEBEVEILIGINGSORGANISATIE

ICT in perspectief

M&I/Partners/

adviseurs voor management en informatie

Leeswijzer

1 **Waarom dit onderzoek?**
Context, aanleiding, uw vraag en onze aanpak

2 **Managementsamenvatting**
Bevindingen en adviezen

3 **Volwassenheidsniveau**
Wat is het huidige volwassenheidsniveau en de ambitie van Arnhem?

4 **Formatie**
Welke formatie is passend bij het huidige volwassenheidsniveau en de ambities?

5 **Frameworks**
Welke risico's en adviezen zien wij aan de hand van het NPCF & BIO?

6 **Bijlagen**
detail NPCF & BIO, geraadpleegde informatie

1

Waarom dit onderzoek?

Context, aanleiding, uw vraag en onze aanpak

WAAROM DIT ONDERZOEK?

1 Context en aanleiding

Het aantal en de ernst van de dreigingen neemt toe
De afgelopen jaren zien we in Nederland (en wereldwijd) de uitdagingen op privacy- & informatiebeveiligingsvlak toenemen. Organisaties krijgen steeds vaker te maken met aanvallen van buitenaf waarbij persoonsgegevens zijn buitgemaakt (Hof van Twente), leveranciers die de regels niet zou nauw nemen (Microsoft), en daarnaast komen ze er ook regelmatig achter dat de eigen medewerkers onbewust veel schade kunnen aanrichten (datadiefstal bij de GGD).

De overheid heeft op het onderwerp privacy een belangrijke voorbeeldrol en een verantwoordelijkheid richting haar inwoners toe om goed om te gaan met persoonsgegevens.

Als gemeenten dit onderwerp structureel de benodigde aandacht willen geven is het van essentieel belang dat gemeenten de organisatie inrichting rondom privacy op orde hebben.

Specifieke aanleiding
De actualiteiten tonen onmiskenbaar aan dat achteroverleunen geen optie is. Daarom wil de gemeente graag een onafhankelijk oordeel van de huidige inrichting en de toekomstbestendigheid hiervan.

WAAROM DIT ONDERZOEK?

1 Dreigingsbeeld Gemeenten IBD

Ambtelijke organisatie	Openbaar bestuur en de politiek	Inwoners en de ondernemers
Bedrijfscontinuïteit	Imagoschade	Gegevens in verkeerde handen
Integriteit van gegevens	Financiële schade	Dienstverlening niet beschikbaar
Gegevens in verkeerde handen	Democratische processen	Ontwrichting van processen

1 Uw vraag en onze aanpak

2

Managementsamenvatting

Bevindingen en adviezen

2 BEVINDINGEN

IB&P draagvlak

Iedereen onderschrijft in gesprekken het belang van IB&P als onderwerp.

Snel opschalen bij calamiteiten

In geval van calamiteiten wordt snel opgeschaald en werkt iedereen mee aan een oplossing.

Stappen gezet

Arnhem is bezig om stappen voorwaarts te zetten op het gebied van informatie-beveiliging en privacy.

Uitgangspunten

Verheldering van uitgangspunten verduidelijkt de verwachtingen die Arnhem en de Connectie over en weer mogen hebben op het gebied van IB&P.

Managementsystematiek ontbreekt

Ontbrekend managementsysteem en lage volwassenheid door ontbrekend beleid.

Bewustzijn vraagt verbetering

Het bewustzijn op het gebied van informatie-beveiliging en privacy in de organisatie vraagt venetering

Formatie informatiebeveiliging & privacy

De formatie is onvoldoende om de structurele werkzaamheden uit te voeren. Achterstanden weg werken vraagt nog extra inzet.

2 Goede basis versterken informatiebeveiliging en privacy

IB&P draagvlak

- Het belang van informatieveiligheid en privacy wordt breed binnen de organisatie gedragen. Dit biedt een goede voedingsbodem om de volwassenheid van informatieveiligheid en privacy te laten groeien door beleid en beheersmaatregelen te versterken.

Snel opschalen bij een calamiteit

- In geval van een calamiteit rond informatiebeveiliging kan de organisatie snel opschalen doordat in samenwerking met de Connectie calamiteitenplannen zijn uitgewerkt**.**

Stappen gezet

- In samenwerking met de Connectie zijn goede stappen gezet om de volwassenheid te verhogen zoals het opstellen van een informatiebeveiligingsplan. Ook wordt er gewerkt aan een regionaal informatie-beveiligingsbeleid.

2 Belangrijkste bevindingen (1/4) - Uitgangspunten

Uitgangspunten op het gebied van privacy en informatiebeveiliging vragen verheldering

- Het consensusmodel in de samenwerking met Rheden en Renkum en Arnhem vertraagt de besluitvorming op kritische elementen in de dienstverlening. Hierdoor loopt het samenwerkingsverband met de Connectie een vergroot risico op het achterblijven van effectieve beveiligingsmaatregelen.
- Op tactisch en operationeel niveau zijn veel processen en procedures onvoldoende beschreven voor het uitvoeren van werkzaamheden op het gebied van informatiebeveiliging en privacy. Hierdoor weten medewerkers niet altijd wat er van hen verwacht wordt. Daarnaast is het moeilijk om te sturen of grip te krijgen op de uitkomsten van deze processen.
- Bij leveranciers is het niet altijd helder of de leveranciers leveren volgens afspraken en of de afspraken aansluiten bij de wensen van de gemeente Arnhem.
- Op het punt van informatiebeveiliging is het niet altijd duidelijk wat Arnhem van de Connectie mag verwachten en vice versa.
  - De **taakverdeling** in termen van taken, bevoegdheden en verantwoordelijken is niet altijd duidelijk waardoor tussen Arnhem en de Connectie er ruis kan ontstaan in de uitvoering van werkzaamheden.
  - Door het ontbreken van **Service Level Afspraken (SLA's)** met de Connectie, kan de Connectie haar dienstverlening minder efficiënt inrichten en krijgt de gemeente mogelijk niet wat ze verwacht.
  - Door het ontbreken van een **dataclassificatie** heeft de Connectie geen helder kaders voor de borging van de informatieveiligheid in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV).
- Het is niet helemaal helder hoe effectief de afstemming is ingeregeld tussen Arnhem en de Connectie op tactisch en operationeel niveau rond informatiebeveiliging.

2 Belangrijkste bevindingen (2/4) – Managementsystematiek

Werkzaamheden op het gebied van privacy en informatiebeveiliging vinden nog grotendeels ad hoc plaats.

- Er is nog geen managementsysteem voor zowel privacy (PIMS) als voor informatiebeveiliging (ISMS)
- De werking van het managementsysteem is voor een groot deel afhankelijk van het goed inrichten en beheren van het zicht op informatieassets en systemen. Voor privacy gaat het hierbij om het verwerkingsregister, DPIA's, verwerkingsovereenkomsten en brede risico-analyses. Voor Informatiebeveiliging gaat het hierbij om Assetmanagement, dataclassificatie (BIA's), risico-analyses en de ENSIA rapportage.
- Er zijn geen heldere rapportagelijnen aanwezig, noch zijn er afspraken over de indicatoren / processen waarover gerapporteerd moet worden. Startpunt hierbij is het definiëren van heldere doelstellingen.
- Er wordt binnen het privacy- en informatieveiligheidsdomein onvoldoende risicogedreven gewerkt. Hierdoor heeft de gemeente geen (gestructureerde) grip op de risico's die zij loopt. Er is wel een start gemaakt met de uitvoering van BIA's en DPIA's. De opvolging van uitkomsten kan hierbij nog helderder worden geborgd.
- Verhogen van het volwassenheidsniveau op gebied van standaard ITIL processen die een nauwe band met informatieveiligheid hebben zoals toegangsbeleid, patchmanagement, incidentmanagement. Wij zien in de praktijk dat een hoog volwassenheidsniveau van ITIL processen leidt tot een hogere effectiviteit op gebied van informatiebeveiliging.

2 Belangrijkste bevindingen (3/4) – Bewustzijn

Het bewustzijn op het vlak van informatiebeveiliging en privacy vraagt verbetering

- Op het gebied van informatiebeveiliging en privacy is het bewustzijn binnen Arnhem laag.
- Er wordt geen extra aandacht besteed aan informatiebeveiliging en privacy bij indiensttreding.
- Er wordt geen periodieke aandacht besteed aan bewustwording, door bijv. campagnes.
- Er zijn geen trainingen beschikbaar op het gebied van informatiebeveiliging en privacy voor medewerkers. Deze zijn niet aangetroffen voor medewerkers die met gevoelige informatie omgaan.
- Er is een oplossing voor beveiligd mailen, maar deze word als erg ingewikkeld ervaren.
- Er is geen wachtwoordkluis. Hier is wel behoefte aan.

2 Belangrijkste bevindingen (4/4) - Formatie

De huidige operationele formatie voor privacy en informatiebeveiliging is onvoldoende.

- De *formatie informatiebeveiliging* is te laag.
  - Het aantal fte voor informatiebeveiliging (0,8 fte) is structureel onvoldoende om informatiebeveiliging op orde te houden. Het op de kaart zetten en instandhouden van informatieveiligheid in de regio-samenwerking vraagt hier veel aandacht. Op het gebied van operationele taken rond informatie-beveiliging (ISO) ontbreekt het structureel aan capaciteit (benchmark[1)] gemiddeld 3,1 fte) .
  - Om de basis op orde te krijgen voor Arnhem is daarbij tijdelijk extra capaciteit nodig.
- De *formatie privacyhuishouding* is te laag.
  - De Functionaris Gegevensbescherming (FG) werkt voor 0,1 fte als FG voor Arnhem. Dit is onvoldoende om de taken van FG goed uit te voeren (benchmark[1)] gemiddeld 0,6 fte).
  - De Privacy Officer (PO) werkt 0,9 fte als PO voor Arnhem en de Connectie. Dit is onvoldoende voor een gemeente met de grootte en complexiteit van die van Arnhem. De PO doet ook werkzaamheden voor de Connectie wat een belangenverstrengeling op kan leveren. (benchmark[1)] gemiddeld 1,5 fte).
  - Om de basis van informatiebeveiliging en privacy op orde te krijgen voor Arnhem is tijdelijk extra capaciteit nodig.

[1)] Benchmark gemeenten informatieveiligheid en privacy bij 100.000+ gemeenten 2020 M&I/Partners/

2 Advies bij bevindingen (1/4) - Uitgangspunten

- Zorg dat kritische processen die gekoppeld zijn aan informatieveiligheid en privacy zijn beschreven en formeel zijn vastgesteld door de organisatie.
- Zorg dat helder is wat leveranciers wordt verwacht en regel daarbij leveranciersmanagement helder in. Hiermee wordt geborgd dat:
  - Arnhem diensten krijgt die aansluiten bij de behoeften van de gemeente en
  - leveranciers leveren wat is afgesproken.
- Creëer meer helderheid over de verwachtingen ten aanzien van dienstverlening en de verdeling van IB&P-taken tussen Arnhem en de Connectie door een heldere opsomming van taken en geef aan wie verantwoordelijk is voor de uitvoering per taak.
- Verhoog het volwassenheidsniveau op gebied van standaard **ITIL processen** die een nauwe band met informatieveiligheid zoals encryptiebeleid, patchmanagement, incidentmanagement. Wij zien in de praktijk dat een hoog volwassenheidsniveau van ITIL processen leidt tot een hogere effectiviteit op gebied van informatiebeveiliging.
- Voer nader onderzoek uit op de effectiviteit van de afstemming rond informatiebeveiliging met de Connectie op tactisch en operationeel niveau.

2 Advies bij bevindingen (2/4) - Managementsystematiek

Zorg voor inrichting van een managementsysteem.

- Breng de grootste risico's op gebied van privacy en informatiebeveiliging in kaart zodat deze gebruikt kunnen worden voor de prioritering van werkzaamheden. Sluit voor de inrichting van risicomanagement aan bij de bestaande risicomanagementprocessen, zoals die van de risk managers.
- Start een project om achterstallig onderhoud weg te werken op gebied van compliance.
  - Besteed expliciet aandacht aan taken, verantwoordelijkheden en bevoegdheden aan betrokkenen bij het managementsysteem.
  - Besteed expliciet aandacht aan het documenteren van procedures, processen en beleid.
- Start het managementsysteem op met één of twee oefen-cycli met begeleiding om de organisatie te laten ervaren hoe het managementsysteem functioneert en waarde toevoegt.
- Pak dit integraal op, dus zowel het privacy information management system als het information security management system zodat er een één systeem ontstaat.
- Zorg voor een brede borging van het managementsysteem in de organisatie; neem belangrijke stakeholders mee in dit proces om breed draagvlak te creëren èn ondersteun de invoering van het managementsysteem op actieve wijze.
- Zorg dat geschreven beleid goed belegd, gedragen en begrepen wordt in de organisatie. Richt hiervoor bijvoorbeeld toetsmomenten in waarop gekeken wordt hoe effectief papier in de praktijk is.

2 Advies bij bevindingen (3/4) - Bewustwording

Stel een plan op voor bewustwordingsacties, zeker op het gebied van privacy.

- Zorg dat medewerkers een duidelijk aanspreekpunt hebben om laagdrempelig vragen aan te stellen dat niet persoonsgebonden is, door bijvoorbeeld naar buiten te treden als het privacyteam.
- Start weer met periodieke bewustwordingsacties, door bijvoorbeeld in te spelen op veel voorkomende datalekken, vragen of actualiteiten. De ISO en de PO zullen deze campagne uitvoeren. De huidige capaciteit hiervoor is te krap.
- Besteed bij indiensttreding specifiek aandacht aan informatiebeveiliging en privacy. Hierbij kan bijvoorbeeld gedacht worden aan een verplichte e-learning waarbij gecontroleerd wordt of deze e-learning gevolgd is.
- Geef training op het gebruik van Cryptshare. Stel duidelijke regels op wanneer Cryptshare gebruikt moet worden.

2 Advies bij bevindingen (4/4) - Formatie

Formatie – tijdelijke uitbreiding

1. Om te zorgen dat de ‘basis op orde’ komt op gebied van informatiebeveiliging en privacybescherming is een investering nodig. Zonder deze investering zal de uitbreiding van formatie beperkt effectief zijn en is er geen solide basis (management systeem) om op voort te bouwen.

2. Baseer de inzet van inzet op de aanname dat van het huidige volwassenheidsniveau de stap gemaakt moet worden naar tenminste volwassenheidsniveau 3 en bij voorkeur niveau 4. De gemeente Arnhem heeft nu veelal een ad hoc aanpak van informatieveiligheid en zit daarbij op niveau 1 (zie hoofdstuk volwassenheidsscores).

3. Als vuistregel geldt dat bij een stijging van 1 procesvolwassenheidsniveau een bijbehorende investering (interne inzet) van +/- 100k. Wanneer we dit plotten voor de SO en PO functie komt dit op ongeveer 200k intern of 400k extern uit per niveaustijging in de volwassenheid.

2 Advies bij bevindingen (4/4) - Formatie

Formatie – structurele inzet

1. **CISO**
   Handhaaf de structurele inzet van de CISO op 1,0 fte.
2. **ISO**
   Breid de formatie van de ISO uit tot van minimaal 2 fte's tot samen maximaal 4,0 fte. De ISO stelt beleid op en voert de operationele informatie-beveiligingstaken uit, zoals het doen van risicoanalyses, assisteren bij audits en het ondernemen van bewustwordingsacties.
3. **FG**
   Voor de FG verwachten we een minimaal benodigde formatie van 0,5 fte (extern) of 1,0 fte (intern). Bij een externe FG gaan we er vanuit dat kennisborging niet binnen de formatie valt waardoor de functie in minder formatie uitgevoerd kan worden. Bij een interne FG wordt dit gedaan in de werktijd voor Arnhem.
4. **PO**
   Zorg structureel voor uitbreiding op de formatie voor de Privacy Officer. Op basis van het onderzoek wordt een minimale inzet van 2,0 fte verwacht. Wanneer volwassenheidsniveau 3 is bereikt zal structurele formatie beter beoordeeld kunnen worden. Dit om de privacy-taken goed te kunnen volbrengen en de organisatie mee te kunnen nemen. De PO kan dan de informatiebeveiligingsorganisatie ondersteunen in een aantal taken die in elkaars lijn liggen, zoals bewustwording, aanhaken bij projecten en het opstellen/bijstellen van procedures.

2 Advies bij bevindingen (4/4) - Formatie

Specialisatie van de ISO en PO rol
De complexiteit van de gemeentelijke processen incl. de bijbehorende wet en regelgeving zorgen dat onze ervaring is dat PO's en ISO's effectiever zijn met een specifieke 'domeinportefeuille'. Hiermee wordt bedoeld dat bijv. een PO op het sociaal domein met specifieke kennis van de context en processen beter kan adviseren en ondersteunen. Naarmate gemeenten groter worden zien we de formatie per domein stijgen. Voor 100+ gemeenten zien we bijv. regelmatig 1 fte PO + 1 fte ISO sociaal domein

3

Scores

Wat is het huidige volwassenheidsniveau en de ambitie van Arnhem?

SCORE

METING INFORMATIEBEVEILIGING

id	onderwerp
5	Informatiebeveiligingsbeleid
6	Organiseren van informatiebeveiliging
7	Veilig personeel
8	Beheer van bedrijfsmiddelen
9	Toegangsbeveiliging
10	Cryptografie
11	Fysieke beveiliging en beveiliging van de omgeving
12	Beveiliging bedrijfsvoering
13	Communicatiebeveiliging
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen
15	Leveranciersrelaties
16	Beheer van informatiebeveiligingsincidenten
17	Informatiebeveiligingsaspecten van bedrijfscontuinuïteitsbeheer
18	Naleving

[redacted]

3 Advies bij scores informatiebeveiliging

Werk de basis voor het informatiebeveiligingsbeleid uit (Governance structuur)

1. Definieer heldere Taken, Bevoegdheden en Verantwoordelijkheden (TBV's)
2. Zorg voor een heldere scope afbakening t.a.v. de baseline en gevraagde dienstverlening.
3. Richt het ISMS (incl. rapportage cyclus) in.
4. Richt het risicomanagement proces in.
5. Borg kritische processen rond informatiebeveiliging i.s.m. de Connectie (via leveranciersmanagement) via "*regel of leg uit en bewaak*", waaronder:
   - Patch management
   - Cryptografiebeleid
   - Incidentmanagement (incl. scenario's)
   - Assetmanagement
   - Wijzigingen beheer
6. Classificeer data en beleg eigenaarschap van processen/toepassingen

SCORE

METING PRIVACY

Onderwerp	Score	Max	Realisatie
1. Privacy management	5	47	11%
2. Privacystatement	0	2	0%
3. Toestemming	0	4	0%
4. Verzamelen	0	1	0%
5. Gebruik, opslag en vernietiging	2	9	22%
6. Rechten van betrokkene en kwaliteit van gegevens	6	18	33%
7. Verstrekken	1	4	25%
8. Informatiebeveiliging			
9. Monitoring en handhaving	0	4	0%
	14	**89**	**16%**

Informatiebeveiliging wordt gemeten onder de BIO

3 Advies bij scores privacy

Werk de basis voor privacy uit

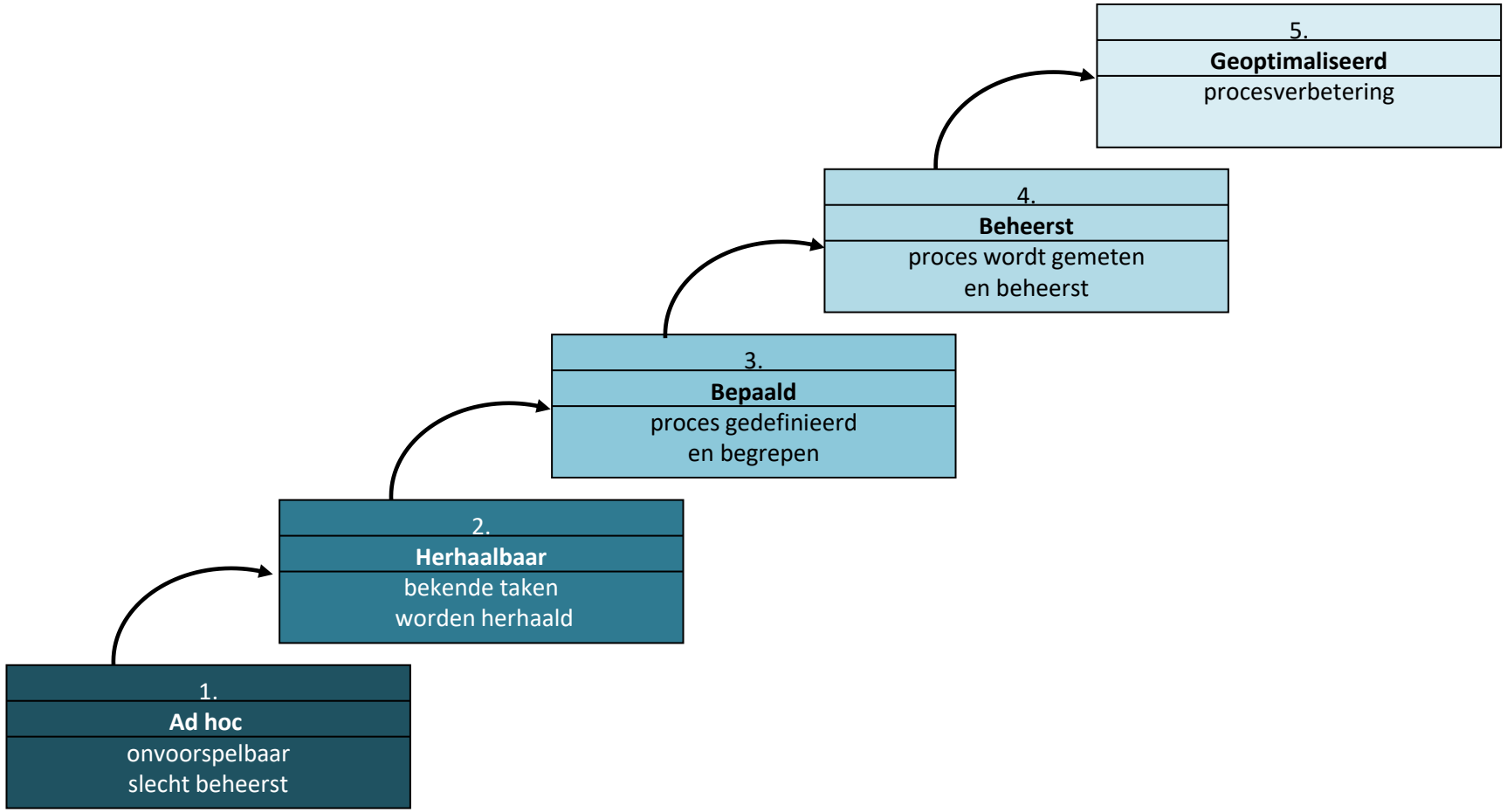
1. Verhelder de taken, bevoegdheden en verantwoordelijkheden (TBV's) op het gebied van privacy
   - Stel hierbij ook vast wie verantwoordelijk is voor de privacy van het sociaal domein en andere uitbestede diensten. Indien dit een mandaatregeling is, zou er voorzichtig omgegaan moeten worden met de privacyborging om belangenverstrengeling te voorkomen.
2. Stel privacyuitgangspunten vast, bepaal het ambitieniveau en tempo
3. Stel een privacybeleid op waarin de uitgangspunten en TBV's worden meegenomen
4. Richt een PIMS in en houdt dit bij gedurende het basis op orde project (incl. rapportagecyclus)
5. Inrichten risicomanagement en opnemen in PIMS
6. Opstellen verwerkingsregister, incl. proceseigenaren, bewaartermijnen, grondslag en of er een DPIA uitgevoerd moet worden op de verwerking of al uitgevoerd is.
7. Start met bewustwordingsacties, focus hierbij eerst op leidinggevenden en op

3

Volwassenheidsniveau

Wat is het huidige volwassenheidsniveau en de ambitie van Arnhem?

3 Volwassenheidsniveau IB&P



Ambitie IB&P – Arnhem.
Beheerst.

Ondergrens IB&P – Arnhem.
Bepaald.

Huidige niveau IB&P – Arnhem.
Initieel, ad hoc en niet voorspelbaar.

Volwassenheidsniveaus ICT organisatie volgens het CMMI

3 Volwassenheidsniveau IB&P bestaand

CMMI-niveau	Toelichting
1. Ad hoc	Chaotisch en ad hoc; problemen worden pas opgelost als ze zich voordoen.
2. Herhaalbaar	De volgende onderdelen worden beheerst: - Basis projectmanagement is ingericht; - Processen worden gepland en volgens plan uitgevoerd, gemeten en gecontroleerd; - Procesdiscipline en commitment blijven onder tijdsdruk gehandhaafd; - Requirements worden gemanaged en configuratiebeheer is ingericht; - De vooraf gedefinieerde requirements worden gerealiseerd met inachtneming van standaarden en kwaliteitsnormen.
3. Bepaald	De ontwikkelprocessen zijn projectoverstijgend ingericht en beschreven, procesverbetering vindt plaats op basis van systematisch meten, evalueren en kennisoverdracht (training). Een geavanceerde vorm van projectmanagement, inclusief risicomanagement, is ingericht.
4. Beheerst	De performance van (een deel van) de processen wordt kwalitatief beheerst en verbeterd en is kwantitatief voorspelbaar.
5. Geoptimaliseerd	Continue procesverbetering en technische innovatie met behoud van alle voorgaande kenmerken.

Behaald
Deels aanwezig
Niet aangetoond

3 Volwassenheidsniveau gewenst – te zetten stappen

CMMI niveau	Toelichting
1. Ad hoc	Dit niveau is reeds behaald.
2. Herhaalbaar	Dit niveau is deels behaald. De onderdelen van de systematiek om daadwerkelijk herhaalbaar (cyclisch) processen uit te voeren zijn onvoldoende in de praktijk doorgevoerd. Hiervoor zijn tenminste de volgende stappen nodig: - Er worden afspraken gemaakt om processen te controleren, uitkomsten te meten en bij te sturen; - Er worden afspraken gemaakt omtrent afwijkingen als gevolg van tijdsdruk of eventuele andere belangen; - Requirements- en configuratiemanagement moeten (beter) systematisch ingericht worden; - Er moet (periodiek) gecontroleerd worden of (projecten)werkzaamheden conform geldende normen, standaarden en wet- en regelgeving worden uitgevoerd. Waar nodig moet dit leiden tot bijsturing/aanpassing van processen; - Risicomanagement is in de basis ingericht zodat prioritering op de juiste manier gemaakt kan worden.
3. Bepaald	Wanneer het voorgaande niveau (bestendig) is behaald, kan ingezet worden op deze stap: - Er wordt integraal gekeken naar ontwikkelprocessen. Verbeteringen vinden plaats op basis van meten, evalueren en kennisuitwisseling; - Risicomanagement wordt naar een hoger niveau gebracht en is integraal onderdeel van projectmanagement; - Project-/portfoliomanagement wordt naar een hoger niveau gebracht, o.a. op gebied van besturing, monitoring en borging.
4. Beheerst	Na behalen van voorgaande niveaus moet voor dit niveau worden ingezet op: - Structurele kwalitatieve beheersing van processen, aangevuld met de mogelijkheid om deze kwantitatief te besturen.
5. Geoptimaliseerd	Dit niveau is beschouwd als buiten ambitie op basis van de uitkomsten van dit onderzoek.

4

Formatie Arnhem

4 Taken en formatie bij Arnhem

In de volgende sheets is de situatie geschetst op basis van een onderzoek bij 100.000+ gemeenten in 2019 en 2020. In veel gevallen is de formatie sindsdien iets gestegen.

Voor de aanvullende formatie zien we een behoefte op twee aspecten: tijdelijk en structureel.

- **Tijdelijk:** Deze formatie richt zich op het wegwerken van het achterstallig onderhoud en het borgen van de managementsystematiek (volwassenheidsniveau 3).
- **Structureel:** Deze formatie richt zich op het draaiend houden van het managementsysteem en het uitvoeren van wettelijk vereiste taken (o.a. DPIA's, beheer verwerkingsregister, etc.)

Nadat dit heeft plaatsgevonden, zal opnieuw geëvalueerd moeten worden hoeveel privacy formatie er nodig is. Een eventuele uitbreiding zal naar verwachting dan zitten op de formatie van de privacy officer.

4 Taken en formatie bij 160.000 gemeenten *)

CISO

Formatie

We zagen bij gemeenten met het inwoneraantal van Arnhem in 2020* een gemiddelde van 3,1 fte voor de informatiebeveiliging (=ISO en CISO tezamen).

* Cijfers uit de ICT-Benchmark voor gemeenten die elk jaar door M&I/Partners uitgevoerd wordt.

Taken

Het takenpakket van de Chief Information Security Officer bestaat in de meeste gevallen uit:

- aanjager van informatiebeveiliging en adviseur op dit gebied voor de directie/CIO, lijnmanagement en de ISO's;
- positieve en actieve houding ten aanzien van informatiebeveiliging;
- stelt meerjarenplan op rondom informatiebeveiliging en bevorderd de informatiebeveiligings-paragraaf in de reguliere jaarplannen van de afdelingen binnen de organisatie;
- toezicht houden op de naleving van informatiebeveiligingsmaatregelen en de naleving van de NEN7510 binnen de gemeente;
- opstellen van verbeterplannen voor het eigen team, uitvoer van deze plannen;
- informatiebeveiliging behandelen in werkoverleg, jaargesprekken, etc.;
- afhandelen van informatiebeveiligingsincidenten;
- controle en registratie, het bewaken van het niveau van informatiebeveiliging van de gemeente;
- communicatie en voorlichting, het coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn bij alle medewerkers;
- coördineren van de interne audit en bijhouden van de resultaten;
- stelt het jaarverslag en tertaalrapportages (=viermaandelijks, wordt vaker gehanteerd) of kwartaalrapportages op rondom informatiebeveiliging met hierin de incidenten, voortgang over het behandelplan en toe te wijzen middelen voor het komende jaar.

*) gemeentes met een vergelijkbaar inwoneraantal.

4 Taken en formatie bij 160.000 gemeenten *)

ISO

Formatie

We zagen bij gemeenten met het inwoneraantal van Arnhem in 2020* een gemiddelde van 3,1 fte voor de informatiebeveiliging (=ISO en CISO tezamen).

* Cijfers uit de ICT-Benchmark voor gemeenten die elk jaar door M&I/Partners uitgevoerd wordt.

Taken

De ISO is verantwoordelijk voor:

- het uitvoeren van risicoanalyses met en adviseren van de proceseigenaren en lijnmanagers van de organisatieonderdelen over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen het organisatieonderdeel;
- het analyseren en beoordelen van de aard, omvang en oorzaak van informatiebeveiligingsincidenten;
- het organiseren van de evaluatie van de afhandeling van informatiebeveiligingsincidenten;
- het adviseren van de organisatie over de te nemen preventieve en herstelacties bij informatiebeveiligingsincidenten;
- het centraal informeren van gebruikers over (potentiële) informatiebeveiligingsincidenten;
- het coördineren van de uitvoering van preventieve en herstelacties;
- rapporteren aan de CISO over de implementatiegraad van de maatregelen die uit de risicoanalyse zijn opgesteld;
- uitvoeren van de interne (intercollegiale) audits bij andere afdelingen over de voortgang van het behandelplan (document met de jaarplanning rondom het verhelpen van risico's).

*) gemeentes met een vergelijkbaar inwoneraantal.

4 Taken en formatie bij 160.000 gemeenten *)

Functionaris Gegevensbescherming

Formatie

We zagen bij 100.000+ gemeenten (2019) een gemiddelde van 0.6 fte voor de functionaris gegevensbescherming, hierbij zit de ondergrens op 0.1 fte en de bovengrens op 1.0 fte.
Om de doelen te realiseren werd een interne formatie onder de 1.0 als ondergrens bestempeld om kennisniveau op peil te houden.

Taken

Het takenpakket van de functionaris gegevensbescherming bestond in de meeste gevallen uit:

- evaluatie en advies, het adviseren van het bestuur, directie en andere leidinggevenden over privacybescherming en het rapporteren over de status van privacybescherming binnen de gemeente;
- m.b.t. AVG en andere privacyregels juridische aanbevelingen doen voor een betere bescherming van verwerkingen van persoonsgegevens;
- het op peil brengen en houden van kennis en bewustzijn rondom gegevensbescherming in de organisatie;
- toezien op de kwaliteit van het register van verwerkingsactiviteiten;
- adviseren bij en controleren van DPIA's;
- adviseren en informeren van medewerkers en inwoners rondom persoonsgegevensverwerkingen;
- Adviseren m.b.t. het afhandelen van datalekken en deze vastleggen in een datalekregister.

De FG heeft veelal een coördinerende rol in deze verantwoordelijkheden en adviseert op strategisch niveau. De FG rapporteert direct aan de directie en voert onafhankelijk zijn taak uit.

*) gemeentes met een vergelijkbaar inwoneraantal.

4 Taken en formatie bij 160.000 gemeenten *)

Privacy officer

Formatie

We zagen bij 100.000+ gemeenten (2019) een gemiddelde van 1.9 fte voor de Privacy Officer, hierbij zit de ondergrens op 0.8 fte en de bovengrens op 4.0 fte.
De gemiddelde formatie (1.9 fte) werd bij een deel van de gemeenten als voldoende ervaren om de ambities waar te maken. Een ander deel gaf aan gezien complexe, vaak regionale, taken behoefte te hebben aan tenminste 3.0 fte.

Taken

Het takenpakket van de Privacy Officer(s) bestond in de meeste gevallen uit:

- De advisering op operationeel niveau ligt veelal bij de Privacy Officer.
- Verantwoordelijk voor afhandeling van (ad hoc) inhoudelijke vraagstukken.
- Communicatie met de vakafdelingen
- Uitvoeren van privacy-gerelateerde projectactiviteiten.
- Coördinatie van de vereiste taken zoals benoemd onder de AVG op operationeel niveau en voert waar nodig ook uit. Onder deze taken vallen onder andere:
  - Bijhouden van het register van verwerkingen;
  - begeleiden van DPIA's;
  - coördineren van rechten van betrokkenen;
  - beheer / onderhoud van het privacy statement en;
  - beheer / onderhoud van het privacybeleid, inclusief het volgen van nieuwe ontwikkelingen en wetgeving.

*) gemeentes met een vergelijkbaar inwoneraantal.

4 Welke bemensing is passend voor een toekomstbestendige privacyorganisatie?

Vaak voorkomende rollen

FG	Functionaris gegevensbescherming: toezichthouder op naleving van privacy wet- en regelgeving
PO	Privacy Officer: uitvoerende medewerker op het gebied van privacy.

Voorgestelde formatie binnen Arnhem

FG	Arnhem heeft een formatie van 0.1 fte op privacy. Dit is onvoldoende om alle taken van de FG uit te voeren. We verwachten dat een formatie van 0.5 fte (extern) of 1.0 fte (intern) nodig is om alle taken structureel uit te kunnen voeren. Hiervoor moet de PO-functie goed ingevuld zijn, zodat de FG een puur toezichthoudende rol kan hebben.
PO	We verwachten dat voor het uitvoeren van de taken van PO er tenminste 2,0 fte nodig is en maximaal 4,0 fte, gezien de complexe, regionale taken die Arnhem heeft. Als hier 2,0 fte twee jaar ingezet zijn, nadat de basis op orde gebracht is, moet opnieuw geëvalueerd worden of dit voldoende is. Hiernaast moeten een aantal zaken verbeterd en opgezet worden. Hiervoor is tenminste 1,0 fte gedurende 1 jaar nodig, eventueel te verdelen over meerdere jaren. Dit vergt dus een investering van ongeveer 200.000 euro.

4 Welke bemensing is passend voor een toekomstbestendige informatiebeveiligingsorganisatie?

Vaak voorkomende rollen

CISO	CISO: bewaking en aansturing van informatiebeveiliging
ISO	ISO: uitvoerende medewerker op het gebied van informatiebeveiliging.

Voorgestelde formatie binnen Arnhem

CISO	We verwachten dat voor het uitvoeren van de informatieveiligheidsrol de huidige formatie minimaal is, mits de afspraken en verwachtingen tussen Arnhem en de Connectie duidelijk zijn en de ISO's een aantal taken van de CISO overnemen/hierbij ondersteunen. Minder dan 1,0 fte voor Arnhem is te weinig om alle taken te doen.
ISO	Er zijn momenteel geen ISO's bij de gemeente Arnhem. Ondanks dat het een en ander op het gebied van informatiebeveiliging belegd is bij de Connectie, heeft Arnhem wel nog eigen verantwoordelijkheden. Om dit goed uit te kunnen voeren is een formatie van 2,0 fte nodig. Hiernaast moeten een aantal zaken verbeterd en opgezet worden. Hiervoor is tenminste 1,0 fte gedurende 1 jaar nodig, eventueel te verdelen over meerdere jaren. Dit vergt dus een investering van ongeveer 200.000 euro.

4 Voorgestelde IB&P organisatieinrichting - minimum

CISO *(1 FTE)*
Taken: Communiceren, adviseren en coördineren rondom informatiebeveiliging

Functionaris Gegevensbescherming *(0,5-1,0 FTE)*
Taken: Toezichthouden, informeren & adviseren

ISO *(1 FTE)*

ISO *(1 FTE)*

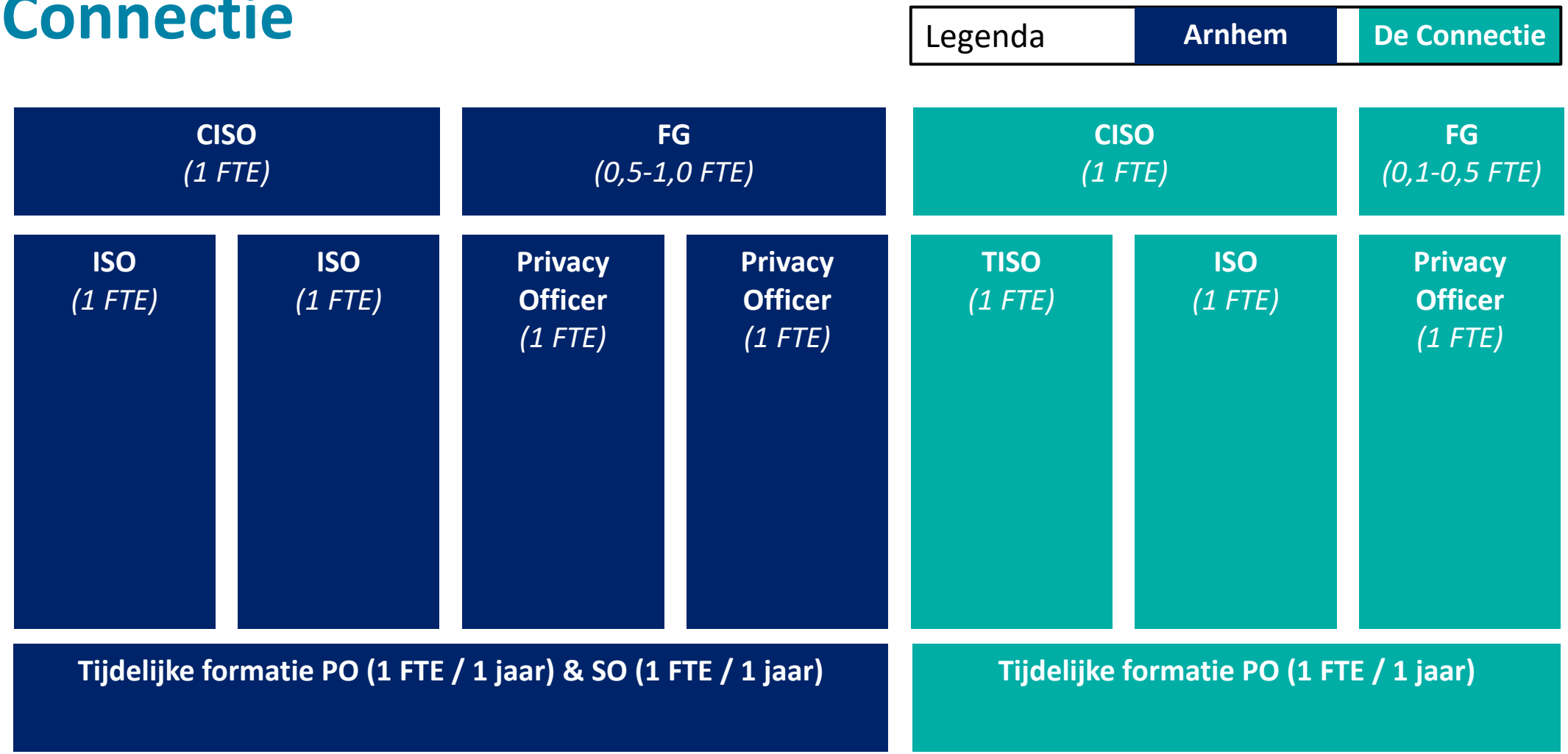
Privacy Officer *(1 FTE)*

Privacy Officer *(1 FTE)*

Tijdelijke formatie PO (1 FTE / 1 jaar) & SO (1 FTE / 1 jaar)
Taken: Basis op orde

FORMATIE ARNHEM

4 Voorgestelde IB&P organisatieinrichting – Arnhem + Connectie



4 Voorgestelde IB&P organisatieinrichting De Connectie

Technical Security Officer (TISO)

Taken

De Technical Security Officer is samen met een security team verantwoordelijk voor de technische aspecten van informatiebeveiliging. Daarbij zal de inzet van nieuwe beveiligingsoplossingen (MS365 diensten en SOC / SIEM) ook vragen om inzet van medewerkers die de beveiligingsmeldingen monitoren, beoordelen en opvolgen.

De TISO is verantwoordelijk voor:

- Beoordelen van technische beveiligingsmaatregelen (o.a. beveiligingsprotocollen, encryptie-algoritmen, IAM, firewalls) voor de ontwerpen van de technische omgeving: netwerk, infrastructuur (zowel cloud als on-premise datacenters), applicaties, SaaS, extern verbindingen, enz.
- Samenwerken met het beveiligingsteam aan een breed scala aan beveiligings- en compliance taken, b.v. periodieke controle, naleving van regelgeving, diepgaande beoordelingen dreigingen, IT-beveiligingstraining en coaching bieden, kwetsbaarheden en beveiligingsincidenten interpreteren op impact voor services, keten-beveiliging, enz.
- In nauwe samenwerking met infrastructuur en applicatiebeheer en eventueel Security Operation Center proactief identificeren en ondersteunen bij het implementeren van de juiste beveiligingsmaatregelen.

5. Norea privacy control framework

5 Norea privacy control framework

Onze kwalitatieve meting is uitgevoerd op basis van het NOREA privacy control framework. Deze bestaat uit 9 categorieën met 103 controls in totaal. Voor deze rapportage is het framework vertaald en zijn voor de context irrelevante controls verwijderd.

Categorie	Subcategorieën	Controls
1. Management	9	47
2. Privacystatement	1	2
3. Toestemming	1	4
4. Verzamelen	1	1
5. Gebruik, opslag en vernietiging	4	9
6. Rechten van betrokkene en kwaliteit van gegevens	5	18
7. Verstrekken	2	4
8. Informatiebeveiliging	5	14
9. Monitoring en handhaving	2	4

5 Norea privacy control framework - Overzicht

	Totaal	Maximaal
	14	103

	Score	Maximaal
1. Privacy management	**5**	**47**
Privacy beleid	2	7
Definities van taken en verantwoordelijkheden	1	7
Identificatie en classificatie van persoonsgegevens	0	4
Risicomanagement	0	5
Data protection impact assessments	0	6
Beveiligingsincidenten en datalekken	2	9
Personeelsvereisten	0	4
Interne bewustwording	0	4
Juridische controle op wijzigingen in wettelijke context	0	1
2. Privacystatement	**0**	**2**
Privacystatement	0	2
3. Toestemming	**0**	**4**
Toestemming	0	4
4. Verzamelen	**0**	**1**
Dataminimalisatie	0	1
5. Gebruik, opslag en vernietiging	**2**	**9**
Privacy architectuur (privacy by design & default)	1	3
Bewaartermijnen	0	1
Verwijdering, vernietiging en archivering	0	2
Gebruik en beperkingen	1	3

	Score	Maximaal
6. Rechten van betrokkene en kwaliteit van gegevens	**6**	**18**
Recht op inzage	3	4
Recht op rectificatie	1	4
Recht op vergetelheid	1	4
Recht op data portabiliteit	1	4
Juistheid en volledigheid van gegevens	0	2
7. Verstrekken	**1**	**4**
Verstrekking van gegevens	0	1
Verwerkers / verwerkersovereenkomsten	1	3
8. Informatiebeveiliging	**0**	**14**
Informatiebeveiligingsprogramma	0	7
Identity and access management	0	1
Veilig verzenden	0	1
Versleuteling en end-point security	0	4
Logging van toegang	0	1
9. Monitoring en handhaving	**0**	**4**
Compliance beoordeling	0	1
Monitoren van privacy controls	0	3

Informatiebeveiliging behandelen we verderop

De volledige uitwerking van het Norea Privacy Control Framework is te vinden in de bijlagen

5

5. BIO

5 Bevindingen Informatiebeveiliging (BIO)

[redacted]

5 Informatiebeveiligingsbeleid
- Aansturing door de directie van de informatiebeveiliging

6 Organiseren van informatiebeveiliging
- Interne organisatie
- Mobiele apparatuur en telewerken

7 Veilig personeel
- Voorafgaand aan het dienstverband
- Tijdens het dienstverband

8 Beheer van bedrijfsmiddelen
- Verantwoordelijkheden voor bedrijfsmiddelen
- Informatieclassificatie
- Behandelen van media

9 Digitale toegangsbeveiliging
- Bedrijfseisen voor Digitale toegangsbeveiliging
- Beheer van toegangsrechten van gebruikers
- Gebruikersverantwoordelijkheden
- Digitale toegangsbeveiliging van systeem en toepassing

10 Cryptografie
- Cryptografie

11 Fysieke beveiliging en beveiliging van de omgeving
- Beveiligde gebieden
- Apparatuur

12 Beveiliging bedrijfsvoering
- Bedieningsprocedures en verantwoordelijkheden
- Bescherming tegen malware
- Back-up
- Verslaglegging en monitoren
- Beheer van technische kwetsbaarheden

13 Communicatiebeveiliging
- Beheer van netwerkbeveiliging
- Informatietransport

14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Beveiligingseisen voor informatiesystemen
- Beveiliging in ontwikkelings- en ondersteunende processen

15 Leveranciersrelaties
- Informatiebeveiliging in leveranciersrelaties
- Beheer van dienstverlening van leveranciers

16 Beheer van informatiebeveiligingsincidenten
- Beheer van informatiebeveiligingsincidenten en -verbeteringen

17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Informatiebeveiligingscontinuïteit

18 Naleving
- Naleving van wettelijke en contractuele eisen
- Informatiebeveiligingsbeoordelingen

[redacted]

6. Bijlagen

1. **NOREA PRIVACY CONTROL FRAMEWORK**
2. **BIO**
3. **GERAADPLEEGDE INFORMATIE**

Norea privacy control framework

6 Quickscanresultaten – Management

6 Quickscanresultaten – Management

Wijzigingen in de wettelijke context

- Binnen het gemeentelijk landschap worden steeds sneller wetten ingevoerd. Arnhem moet hier een goed beeld van hebben om te bepalen wat de impact hiervan is op o.a. de privacy organisatie. Dit zou, in elk geval voor privacy, formeel belegd moeten worden.

Bewustzijn

- Uit de interviews viel op dat het bewustzijn bij een aantal medewerkers een zorg is.
- Er is geen gestandaardiseerde methode voor bewustwording. Er werd verwezen naar bewustwordingstrainingen die in het verleden gehouden zijn, maar deze zijn al geruime tijd niet meer gegeven.
- Bij indiensttreding wordt geen aparte aandacht besteed aan privacy.

Personeelsvereisten

- Er worden geen additionele eisen gesteld aan of trainingen vereist van het personeel voor zij met persoonsgegevens aan de slag mogen. Er wordt enkel verwezen naar de VOG die soms, vooral voor nieuwe medewerkers, opgevraagd wordt. Dit is een magere eis, zeker voor functies die met gevoelige data omgaan (jeugd).

Beveiligingsvereisten en datalekken

- Er is een algemeen datalekkenprocedure (stroomdiagram), deze is erg summier en wordt niet jaarlijks herzien. De geleerde lessen worden ook niet gebruikt als input voor awareness trainingen.
- De verantwoordelijkheden van de FG worden niet duidelijk beschreven in de procedure datalekken.

DPIA's

- Er is geen vaste methodiek om DPIA's uit te voeren en deze worden momenteel ook nog beperkt uitgevoerd.

Risicomanagement

- Risicomanagement is een essentieel onderdeel van voldoen aan de AVG. Er wordt aan risicomanagement gedaan, maar deze zijn voornamelijk financieel gedreven. Het privacy risicomanagement sluit hier onvoldoende op aan. Er is ook geen risk appetite gedefinieerd.

6 Quickscanresultaten – Management

Identificatie en classificatie van persoonsgegevens

- Er is een verwerkingsregister. Het register dat er is, is incompleet, verouderd en (op onderdelen) onjuist. Het register zou periodiek bijgewerkt moeten worden en om het register juist te houden zou dit opgenomen kunnen worden in het PIMS. Belangrijk hierbij is ook om periodiek bewustzijn te creëren bij medewerkers zodat zij nieuwe verwerkingen ook gaan herkennen. Bij het starten van nieuwe projecten zou er aandacht moeten zijn voor de mogelijkheid tot het wijzigen van het verwerkingsregister. Dit moet ook de start zijn voor het uitvoeren van DPIA's, het afsluiten van overeenkomsten en het doen van dataclassificatie.

Definities van taken en bevoegdheden

- De rollen en taken van de privacy organisatie en van individuele medewerkers ten aanzien van privacy vragen verheldering. In de eerste lijn weten medewerkers daardoor niet altijd wat er van hen verwacht wordt. In de derde lijn zijn de taken van de FG ook niet altijd helder. Hierdoor kan er rolvermenging ontstaan met bijvoorbeeld de PO en CISO.
- De formatie van FG en PO zijn onvoldoende hun rol goed uit te kunnen voeren.
- Het is niet zeker of met alle verwerkers een verwerkersovereenkomst is afgesloten, vooral voor de kleinere applicaties is dit niet duidelijk. Afspraken rondom verwachtingen van en naar leveranciers (waaronder De Connectie) zijn ook niet duidelijk.

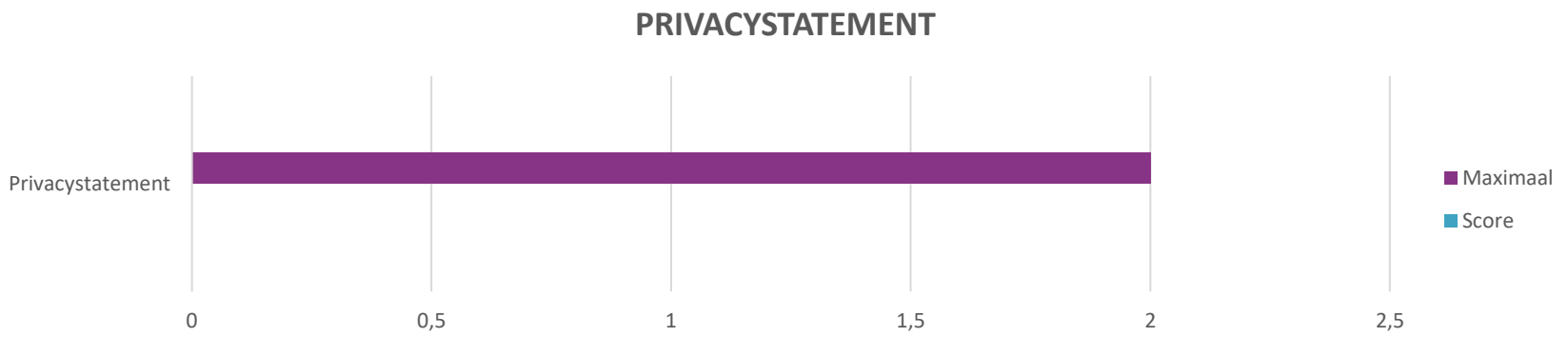
Privacy beleid

- Het privacy beleid is aanwezig, maar verouderd. Het bijhouden en vaststellen moet opgenomen worden in de management cyclus.
- Het verwerkingsregister is niet volledig en niet up-to-date. Er is geen beheerproces ingericht.

Advies:

Prioriteit	• Richt een managementsystematiek in o.a. voor wettelijke ontwikkelingen, privacy beleid, privacy statement, verwerkingsregister, bewustzijn, datalekkenprocedure. Hiervoor moeten eerst de achterstanden worden weggewerkt. Laat het ISMS en het PIMS op elkaar aansluiten.
	• Schenk bij indiensttreding ook aandacht aan privacy, zeker voor functies die met (veel) persoonsgegevens aan de slag gaan.
	• Ontwikkel een standaard DPIA-methode
Prioriteit	• Zorg voor een duidelijke beschrijving van taken, bevoegdheden en verantwoordelijkheden van de FG en voor voldoende formatie op de FG- & PO-functie.
Prioriteit	• Richt risicomanagement op, op het gebied van privacy. Sluit hiervoor aan bij de bestaande risicomanagementmethode, zoals bij financiën, zodat dit integraal opgepakt kan worden. Stel ook een risk appetite vast.
Prioriteit	• Werk het verwerkingsregister bij zodat het up-to-date is en er een duidelijk beeld is welke verwerkingen er plaats vinden.
Prioriteit	• Start weer met bewustwordingsacties rondom privacy (en informatiebeveiliging)

6 Quickscanresultaten – Privacystatement



Privacystatement

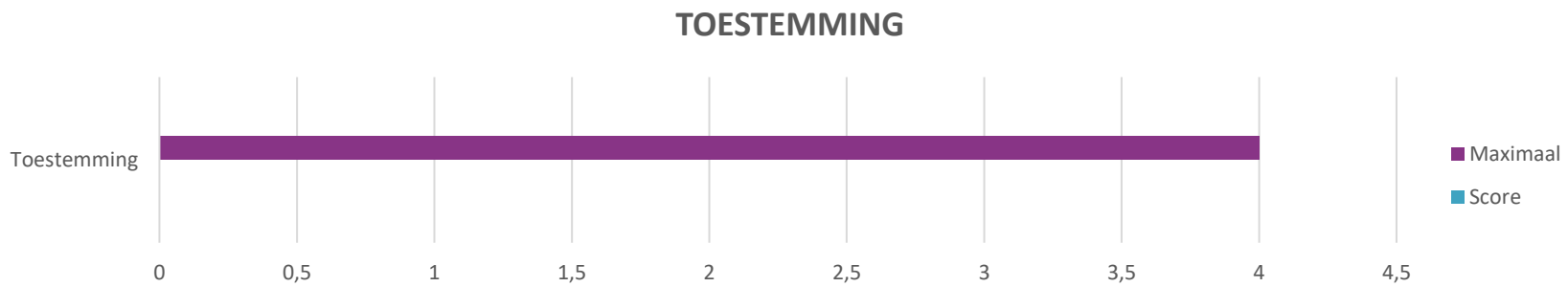
- Het privacystatement is beschikbaar op de website en bestaat dus. Het is echter erg summier. Zo is het bijvoorbeeld niet duidelijk welke gegevens verwerkt worden en waar deze vandaan komen.
- Ook is het onduidelijk wanneer dit statement voor het laatst bijgewerkt is, en dus of het actueel is en of er wijzigingen hebben plaatsgevonden door het ontbreken van een datum.

Quick win

Advies:

- Maak of update het privacy statement, beleg het onderhoud hiervan en neem het op in het PIMS.
- Zorg ervoor dat het duidelijk is wanneer het privacy statement is gewijzigd.

6 Quickscanresultaten – Toestemming



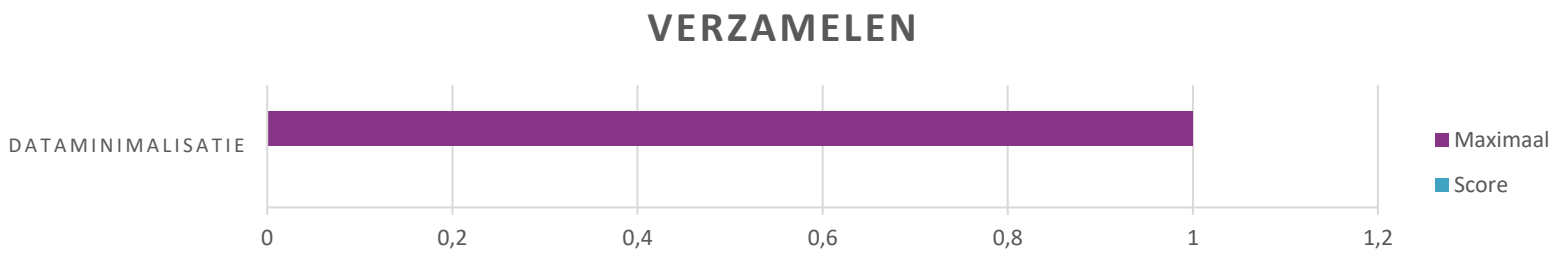
Toestemming

- Voor veel zaken die door Arnhem afgehandeld moeten worden zijn wettelijke gronden van toepassing. Dit onderdeel is dus grotendeels niet van toepassing op de situatie van Arnhem.
- Er wordt wel om toestemming gevraagd aan inwoners om bij het internetpanel te zitten. Deze toestemming is intrekbaar. Het is onduidelijk of medewerkers dit ook weten.

Advies:

•Zorg ervoor dat medewerkers weten wanneer wel om toestemming gevraagd wordt en hoe betrokkenen dit kunnen intrekken.

6 Quickscanresultaten – Verzamelen



Dataminimalisatie

- Er zijn geen (structurele) controls ingericht om te voldoen aan het principe van dataminimalisatie.

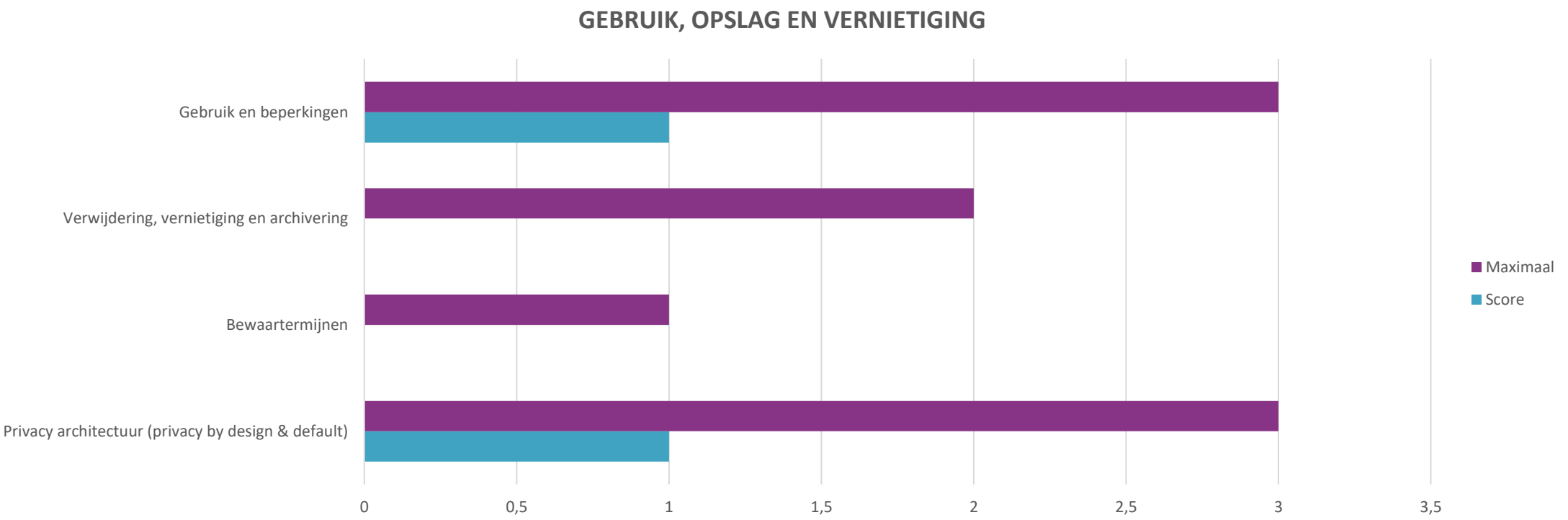
Er kan gedacht worden aan de volgende controls om dit wel te doen:

- Bij iedere nieuwe verwerking beoordelen wat noodzakelijke en optionele gegevens zijn en een bewuste keuze maken in de te verwerken persoonsgegevens. Hiervoor moeten nieuwe verwerkingen als zodanig herkent worden (zie het onderdeel management).
- Periodieke analyses uitvoeren op verwerkingen om te beoordelen of er meer dan de minimaal vereiste set aan persoonsgegevens verwerkt wordt.
- Periodiek analyseren wat de noodzaak is van de verwerking van specifieke persoonsgegevens.

Advies:

- Richt controls in om te voldoen aan dataminimalisatie en neem deze op in het management systeem.

6 Quickscanresultaten – Gebruik, opslag en vernietiging



6 Quickscanresultaten – Gebruik, opslag en vernietiging

Gebruik en beperkingen

- Rechten van betrokkenen zijn duidelijk gecommuniceerd via de website en hier wordt ook gebruik van gemaakt door betrokkenen. Hier is geen proces voor ingericht.

Verwijdering, vernietiging en archivering

- Procedures op het gebied van verwijdering, vernietiging en archivering van informatie ontbreken. Dit zou in het management systeem opgenomen kunnen worden om te zorgen dat dit proces een duidelijke plek binnen de organisatie heeft en om de steekproeven te borgen.

Bewaartermijnen

- Bewaartermijnen zijn per verwerking in het verwerkingsregister opgenomen.
- Informatie na deze bewaartermijnen wordt niet altijd vernietigd en hier wordt ook niet op gecontroleerd. Niet alle systemen hebben de mogelijkheid om dit überhaupt in te kunnen stellen, laat staan automatisch.
- Sommige afdelingen gebruiken andere opslag, bijv. een netwerkschijf, bewaartermijnen worden hierop niet toegepast. Dit geeft ook risico's voor het volledig en juist uitvoeren van de rechten van betrokkenen.

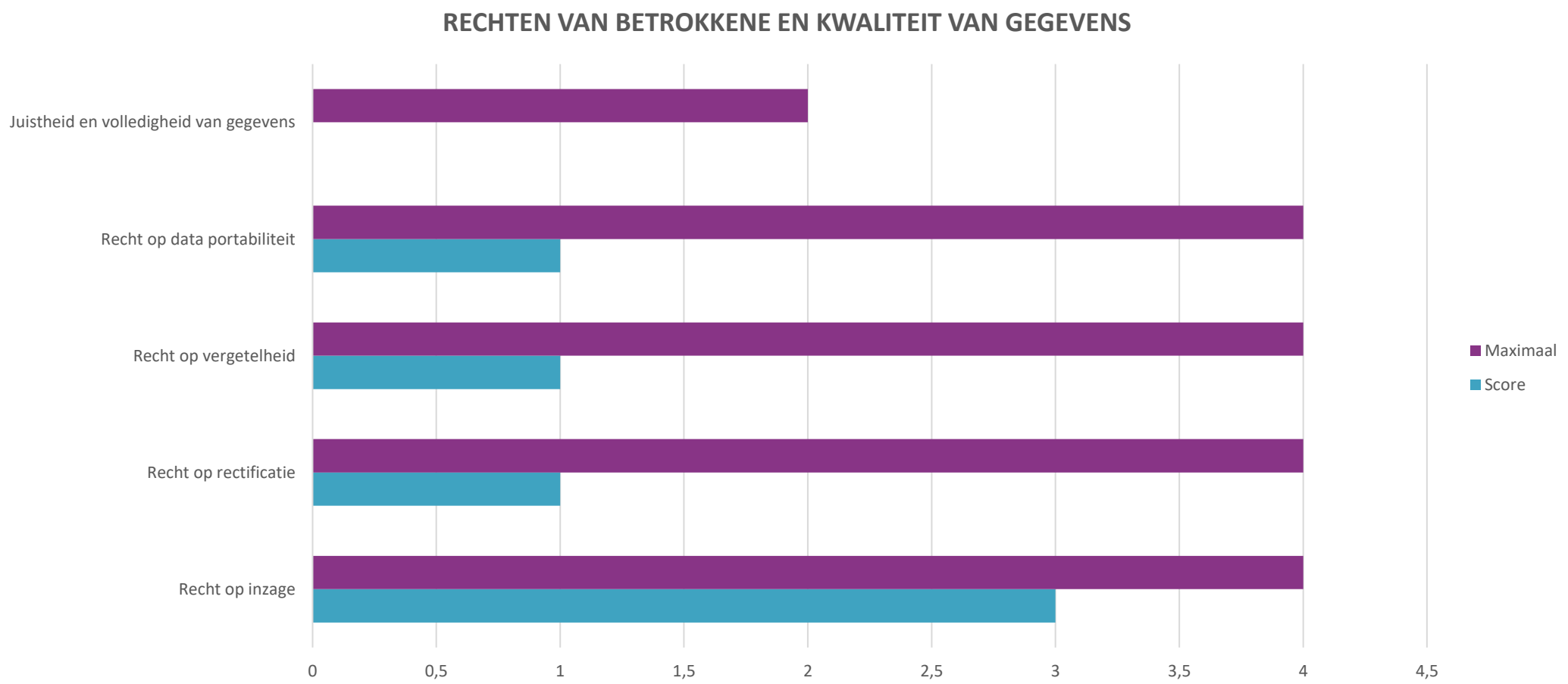
Privacy architectuur

- Bij de inkoop wordt rekening gehouden met privacy by design. Dit is niet altijd het geval bij grote wijzigingen, ook omdat de afspraken rondom privacy niet altijd duidelijk zijn.
- De privacy organisatie wordt niet altijd aangehaakt bij de start van projecten.

Advies:

- Zorg ervoor dat de privacy organisatie ook wordt aangehaakt bij de start van projecten.
- Neem de procedure rechten van betrokkenen, verwijdering, vernietiging en archivering en periodieke controle op bewaartermijnen op in het managementsysteem
- Zorg ervoor dat het ook mogelijk wordt om alle gegevens te verwijderen nadat de bewaartermijn is verstreken
- Overweeg een beheerd alternatief te zoeken voor de losse opslagmogelijkheden.

6 Quickscanresultaten – Rechten van betrokkenen en kwaliteit van gegevens



6 Quickscanresultaten – Rechten van betrokkenen en kwaliteit van gegevens

Juistheid en volledigheid van gegevens

- Er is geen procedure aanwezig om persoonsgegevens te controleren bij verzameling, creatie of onderhoud en daarna periodiek.

Recht op dataportabiliteit

- Dit recht is zelden van toepassing op een gemeente. Hier volstaat een ad hoc aanpak zoals de gemeente hanteert. (In AVG art. 20 Recht op overdraagbaarheid van gegevens bestaat dat recht wanneer de verwerking gebeurt op de grondslag toestemming of de grondslag uitvoering van een overeenkomst. Dat is voor de gemeente zelden het geval.) Wellicht is het wel handig te beschrijven in welke *uitzonderings*situaties dit recht wel van toepassing is.

Recht op vergetelheid

- Er is geen procedure beschreven. Hierdoor is er kans op fouten door de ad hoc aanpak en is de continuïteit niet geborgd.
- Gegevens worden niet automatisch verwijderd na de bewaartermijn, verwijdering is niet altijd mogelijk is.

Recht op rectificatie

- Er is geen procedure beschreven. Hierdoor is er kans op fouten door de ad hoc aanpak en is de continuïteit niet geborgd.

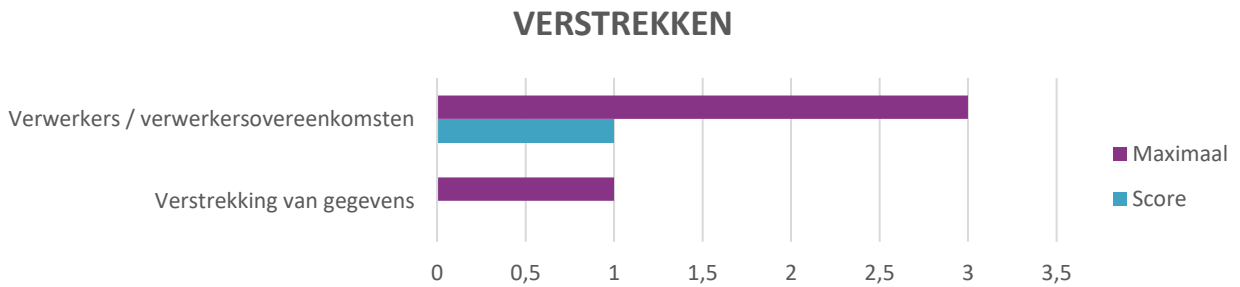
Recht op inzage

- Er is geen procedure beschreven. Hierdoor is er kans op fouten door de ad hoc aanpak en is de continuïteit niet geborgd.

Advies:

- Documenteer bovenstaande zaken en neem het op in het management systeem, beleg dit in de organisatie.

6 Quickscanresultaten – Verstrekken



Verwerkers / Verwerkersovereenkomsten

- Er is geen compleet en correct overzicht van verwerkers en verwerkersovereenkomsten. Dit sluit aan bij de constatering bij de sheet management.
- Er is niet met elke verwerker een verwerkersovereenkomst afgesloten
- Er zijn geen duidelijke afspraken gemaakt met de Connectie over haar dienstverlening.

Verstrekking van gegevens

- Er is geen procedure aanwezig voor het verstrekken van gegevens aan derden. Deze procedure moet opgesteld worden en medewerkers moeten hierop getraind worden.

Advies:

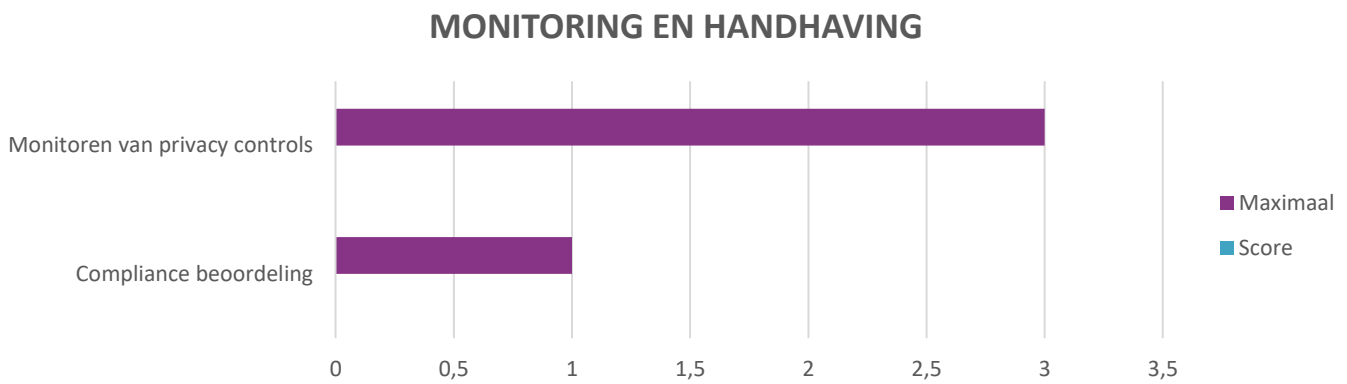
- Zorg dat het overzicht van verwerkers en verwerkersovereenkomsten bijgewerkt wordt en compleet is.
- Maak procedures voor het verstrekken van gegevens aan derden en train medewerkers hierop. Neem dit op in het managementsysteem en beleg dit.
- Maak duidelijke afspraken met de Connectie over de taken, verantwoordelijkheden en bevoegdheden van beide partijen.

Prioriteit

6 Quickscanresultaten – Informatiebeveiliging

Zie BIO.

6 Quickscanresultaten – Monitoring en handhaving



Monitoren van privacy controls

- Er vindt geen structurele monitoring en rapportage plaats op de verschillende privacy controls. Rapportage op specifieke controls kan periodiek opgenomen worden in het managementsysteem.

Compliance beoordelingen

- Er vindt geen structurele beoordeling plaats op compliance op de AVG. Periodieke beoordeling kan opgenomen worden in het PIMS.

Advies:

- Maak rapportages op privacy controls en neem dit op in het PIMS.
- Voer periodieke beoordeling van de AVG compliance uit en neem dit op in het PIMS.

6

6. BIO

BIO

6 Informatiebeveiligingsbeleid

BIO

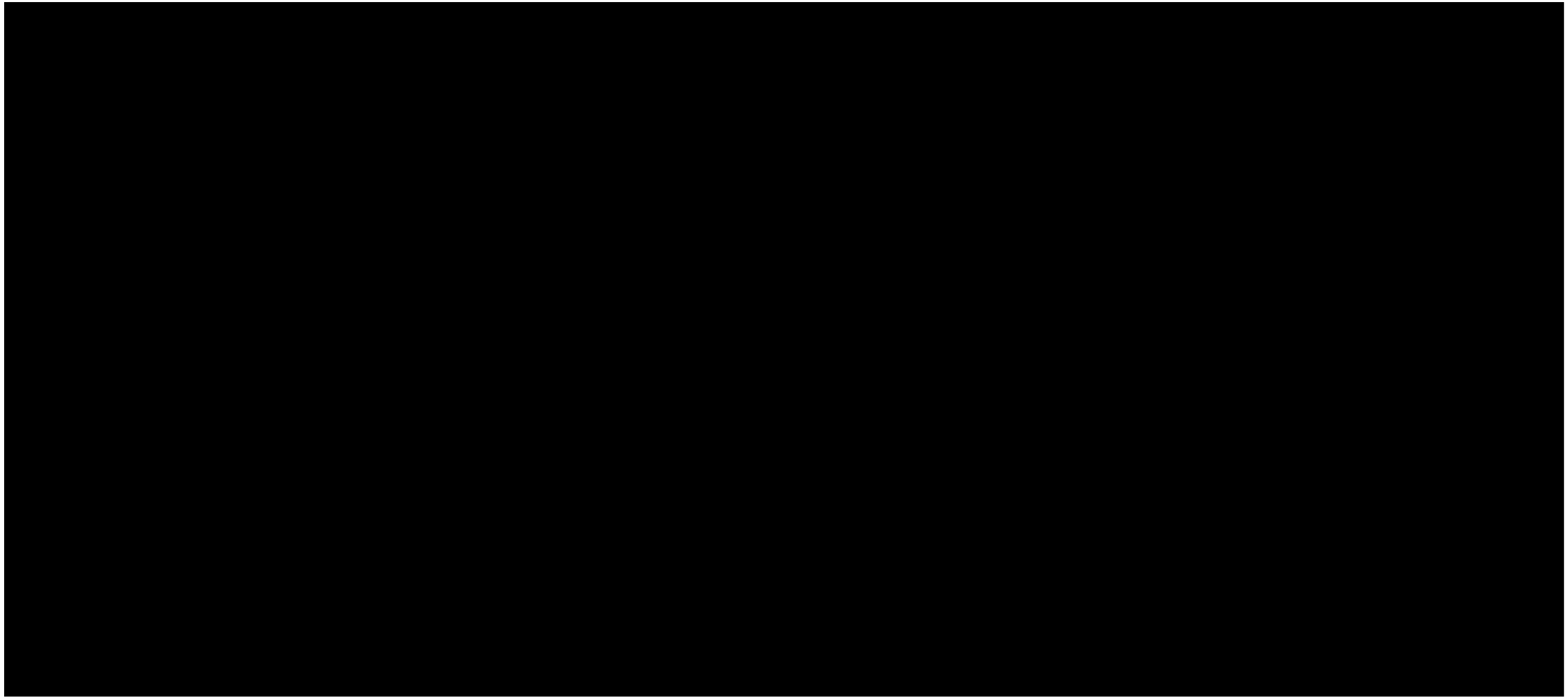
6 Organiseren van informatiebeveiliging

BIO

6 Veilig personeel

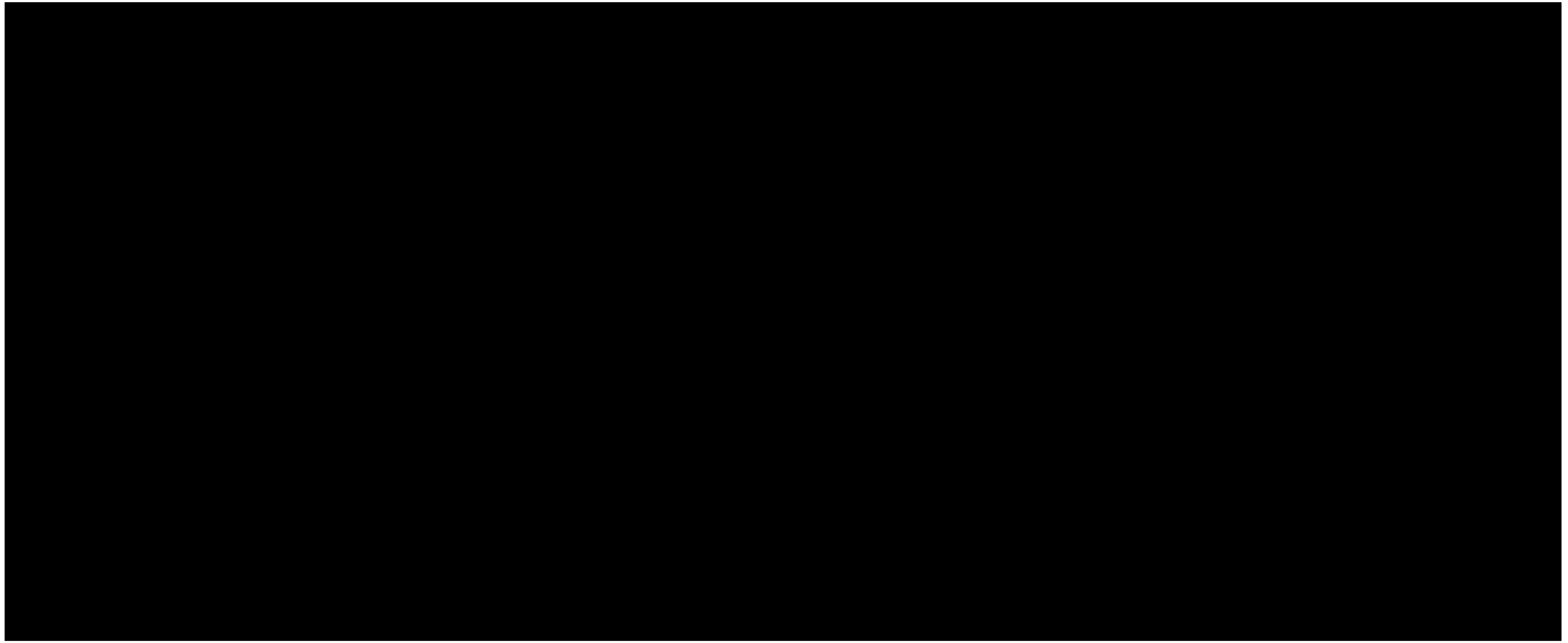
BIO

6 Beheer van bedrijfsmiddelen



BIO

6 Digitale toegangsbeveiliging



BIO

6 Cryptografie

6 Fysieke beveiliging en beveiliging van de omgeving

BIO

6 Beveiliging bedrijfsvoering

BIO

6 Beveiliging bedrijfsvoering

BIO

6 Communicatiebeveiliging

6 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

BIO

6 Leveranciersrelaties

BIO

6 Beheer van informatiebeveiligingsincidenten

BIO

6 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

BIO

6 Naleving

Geraadpleegde informatie

1. **GESPROKEN MEDEWERKERS**

2. **GERAADPLEEGDE DOCUMENTEN**

6 Gesproken medewerkers

6 Geraadpleegde documenten

De volgende documenten zijn bekeken:

1. Algemeen privacybeleid raad Arnhem
2. Autorisatiebeheersproces v1.0 2020-09-28
3. Eindrapportage Privacy en informatieveiligheid in het sociaal domein van de gemeente Arnhem
4. FW Dataclassificatie Szeebra
5. Hardening-proces-definitief
6. Incidentmanagement-procesbeschrijving
7. Kopie van Arnhemse applicaties totaaloverzicht 20220224
8. Notitie privacy sociaal domein
9. 4. De Nota Risicomanagement en weerstandsvermogen van 12 mei 2020
10. 220224 Informatie rondom aanlevering documentatie
11. 20220215 Configuration Management Plan v0.01
12. Patchmanagementproces-definitief
13. Procesbeschrijving-Change-Management-v-3.3
14. Proces-Problem-Management-v1.00
15. Raadsbrief 23122014 bij beleid privacy Sociaal Domein
16. Reactie op isea 3402 aanvraag
17. 190326 DPIA Rapport IRMA app Nijmegen (1.0)
18. bijlage 1 behorende bij overeenkomst gegevensverwerking arnhem renkum rheden de connectie
19. Memo afhandeling beveiligingsincident met zaaknummer 636050
20. ondertekende overeenkomst gegevensverwerking arnhem renkum rheden de connectie
21. Overeenkomst gegevensverwerking Arnhem - Stichting sociale Wijkteams
22. RegistratieOverzicht
23. Stroomschema beveiligingsincidenten
24. Stroomschema datalek
25. Stroomschema datalekken antwoorden
26. VNG Standaard Verwerkersovereenkomst v2.2 aangepast Ah DC

M&I/Partners
M&I/Partners is een onafhankelijk ICT-adviesbureau in de publieke sector met ongeveer 100 professionals. Wij hebben meer dan 35 jaar ervaring in het adviseren en begeleiden van klanten bij projecten op het snijvlak van management en ICT en kiezen voor opdrachten met maatschappelijke meerwaarde.

Als partner werken wij samen aan de realisatie van de maatschappelijke opdracht van onze klanten, door ons advies over een weloverwogen inzet en eventuele implementatie van impactvolle digitalisering en ICT.

Ontdek meer op www.mxi.nl