DATUM	11 december 2024	PLAATS	Twentehuis, 501-503	TIJDSTIP	10.45-12.45
VOORZITTER	C. Bruggink	SECRETARIS	S. Dinsbach	PAGINA	1

GENODIGDEN E. van Mierlo (Almelo), M. Geerdink (Borne), R. de Way (Dinkelland), H. Vedder (DB-lid, Enschede), P. van Zwanenburg (Haaksbergen), L. de Waard (Hellendoorn), C. Bruggink (Hengelo), H. Rohaan (Hof van Twente), M. Oosterbroek (Losser), M. Rödel (Oldenzaal), B. Beens (Rijssen-Holten), H. Berning (Tubbergen), M. Paters (DB-lid, Twenterand), H. ter Keurst (Wierden)

Geïnteresseerden van de vergadering kunnen deze bijwonen in het Twentehuis, 501-503

Agenda algemeen bestuur van 11 december 2024 (reg.nr. 2024-000021)

NR.	ONDERWERP	VOORSTEL/ADVIES	BESLUIT
1	Opening vergadering	Welkom bij de AB vergadering. Er is ook besloten deel van de vergadering. Hiervoor staat de agenda in de afgesloten map op extranet.	
2	Vaststellen agenda		
3	Mededelingen	Stand van zaken kerntakendiscussie	
A - Hamerstukken			
A1	Besluitenlijst AB 13 november 2024	1. Vast te stellen	
B- Bespreekstukken			
B1	Vergoeding voor kosten inzet Jeugdgezondheidszorg (JGZ) t.b.v. Oekraïense vluchtelingen	1. De rijksbijdrage, die de gemeenten ontvangen voor de taken van de JGZ voor Oekraïense vluchtelingen, via separate facturatie bij de gemeenten in rekening te brengen.	
B2	Nota integraal risicomanagement en weerstandsvermogen	1. De nota “Integraal risicomanagement en weerstandsvermogen 2024-2027” vast te stellen. 2. De oude nota “Van risicomanagement tot weerstandsvermogen 2018” in te trekken.	
C – Stukken ter informatie			

NR.	ONDERWERP	VOORSTEL/ADVIES	BESLUIT
C1	Beleidsstukken informatiemanagement, -beveiliging en privacy	Kennis te nemen van 1. Het Informatiebeleidsplan 2025-2028. 2. Het Informatiebeveiligingsbeleid 2025-2028. 3. Het privacybeleid 2025-2028.	
D – Rondvraag en sluiting			

DATUM	13 november 2024	PLAATS	Twentehuis, 501-503	TIJDSTIP	10.15 -11:00
VOORZITTER	C. Bruggink	SECRETARIS	S. Dinsbach	PAGINA	1

AANWEZIGEN: E. van Mierlo (Almelo), M. Geerdink (Borne), R. de Way (Dinkelland), H. Vedder (DB-lid, Enschede), P. van Zwanenburg (Haaksbergen), L. de Waard (Hellendoorn), C. Bruggink (Hengelo), H. Rohaan (Hof van Twente), M. Oosterbroek (Losser), B. Beens (Rijssen-Holten), H. Berning (Tubbergen), M. Paters (DB-lid, Twenterand), H. ter Keurst (Wierden)

AFWEZIG: M. Rödel (Oldenzaal),

Concept besluitenlijst algemeen bestuur van 13 november 2024

NR.	ONDERWERP	VOORSTEL/ADVIES	OPMERKINGEN
1	Opening vergadering	Er is ook besloten deel van de vergadering. Hiervoor staat de agenda in de afgesloten map op extranet.	Voorzitter Claudio Bruggink heet de leden van het AB en de aanwezigen op de publieke tribune welkom en opent de openbare vergadering. Aansluitend volgt nog een besloten deel. Maaike Rödel (Oldenzaal) heeft zich afgemeld. Loes de Haan is afwezig in verband met ziekte. Tineke Hinrichs vervangt haar voorlopig.
2	Vaststellen agenda		De agenda wordt ongewijzigd vastgesteld.
3	Mededelingen	Stand van zaken kerntakendiscussie	<u>Stand van zaken kerntakendiscussie:</u> Hilde Berning (voorzitter van de bestuurlijke begeleidingscommissie kerntakendiscussie) verwijst de AB-leden naar de mail die zij hebben ontvangen over de stand van zaken van de kerntakendiscussie. Daarin wordt de lijn richting besluitvorming op uiterlijk 31 maart 2025 geformuleerd. Er zijn geen vragen vanuit het AB.

NR.	ONDERWERP	VOORSTEL/ADVIES	OPMERKINGEN
			Academische Werkplaats Jeugd Twente (AWJT): Marian Oosterbroek vraagt als bestuurlijk trekker aandacht voor de Academische Werkplaats Jeugd Twente (AWJT) en de nieuwe subsidiecall. Bedoeling is om de sociale basis te versterken vanuit het pedagogisch klimaat. Marian Oosterbroek stuurt de informatie hierover aan de AB-leden. Als het AB geïnteresseerd is kan AWJT wellicht eens worden geagendeerd. Harmjan Vedder vraagt dan wel de verbinding met de Samenwerkingsagenda hierin mee te nemen. Team AnderS: Pieter van Zwanenburg geeft een update over Team AnderS. Dit is een team van intensief ambulante specialisten die ad hoc en kortdurend ingezet worden ter voorkoming van uithuisplaatsing of terugkeer naar huis. De inzet van het team moet nog groeien en is ook wat vertraagd door problemen in de personele bezetting. Er volgt nog een memo met nadere informatie waarin ook wordt opgenomen wat er van de bestuurders wordt verwacht. Wellicht kan ook dit punt op termijn worden geagendeerd voor het AB. Wordt vervolgd.
A - Hamerstukken			
A1	Besluitenlijst AB 16 oktober 2024	1. Vast te stellen	De besluitenlijst wordt ongewijzigd vastgesteld.
A2	Technische begrotingswijziging najaar 2024	1. De lasten en de baten van de programmabegroting 2024 te verhogen met afgerond € 5,49 miljoen en hiervoor de	**Besluit AB:** conform.

NR.	ONDERWERP	VOORSTEL/ADVIES	OPMERKINGEN
		bijgevoegde technische begrotingswijziging vast te stellen.	
A3	Technische begrotingswijziging 2025	1. De lasten en de baten van de programmabegroting 2025 te verhogen met afgerond € 3,73 miljoen en hiervoor de bijgevoegde technische begrotingswijziging vast te stellen.	**Besluit AB:** conform.
B- Bespreekstukken			
B1	Tweede Bestuursrapportage 2024	1. De tweede Bestuursrapportage 2024 vast te stellen.	Harmjan Vedder (portefeuillehouder Bedrijfsvoering) leidt de 2e Berap kort in. Met dank aan de oplettendheid van de gemeente Wierden wordt nog een fout rechtgezet: een te verwachten incidenteel tekort van € 46.000 door lagere opbrengsten bij de inspecties kinderopvang is abusievelijk in de tabel op pagina 15 weggevallen maar het bedrag is wel opgenomen in het totaal bedrag van GGD Twente en op pagina 18 is deze ontwikkeling ook tekstueel toegelicht. Qasim Bajwa (concern controller) licht de berap inhoudelijk toe door middel van een presentatie. De verbetering van de beleidsrealisatie zet zich ook in deze tweede Berap door. Ten opzichte van de eerste Berap 2024 verwachten we meer van onze doelen volledig te kunnen realiseren. Deze verbeteringen zijn zichtbaar bij GGD Twente en Veilig Thuis Twente.

NR.	ONDERWERP	VOORSTEL/ADVIES	OPMERKINGEN
			Er wordt een klein positief resultaat verwacht voor 2024. Zorgelijk is dat er een structureel tekort van 1,5 miljoen per jaar is dat incidenteel gedekt wordt. Het AB uit zijn complimenten voor het heldere verhaal van Qasim en deelt zijn zorg. Men is zich er ook van bewust dat naast de structurele component er meer aspecten zijn die aandacht behoeven zoals de kerntakendiscussie. **Besluit AB:** conform.
C – Stukken ter informatie			
C1	Statusupdate Ontwikkelagenda en implementatie tarief Jeugdbescherming/jeugdreclassering (JBJR)	Kennis te nemen van: 1. De monitoringsafspraken over het landelijk tarief JBJR. 2. De stand van zaken en gewijzigde opdracht van het project Toewijzen. 3. De stand van zaken en gewijzigde opdracht van het project Strategische HR-Agenda.	Portefeuillehouder Mark Paters licht toe dat het project Ontwikkelagenda in de afrondende fase zit en eind 2024 afloopt. De projectgroep heeft te maken gehad met verschillende obstakels, waaronder het gebrek aan draagvlak in de regio IJsselland voor o.a. het (sub)project Toewijzen. Hierdoor wordt er in de laatste fase van het project gekozen voor een andere manier van aanpak om nog zoveel mogelijk te kunnen bewerkstelligen voordat het project afloopt. Om deze reden ligt de informatienota voor aan de opdrachtgever (DB) en het AB om ze te informeren over de wijzigingen in het project. In de evaluatie die later volgt en wordt geagendeerd voor het AB, zal het inhoudelijke effect van het project worden belicht. **Besluit AB:** conform.
C2	Ingekomen brief over tariefsverlaging JeugdGGZ	1. Kennis te nemen van de brief	**Besluit AB:** conform.

NR.	ONDERWERP	VOORSTEL/ADVIES	OPMERKINGEN
C3	Ingekomen brief GS over toezichtsvorm SamenTwente	1. Kennis te nemen van de brief	**Besluit AB:** conform.
D – Rondvraag en sluiting			
			Er wordt geen gebruik gemaakt van de rondvraag. De voorzitter vraagt het publiek de vergaderzaal te verlaten in verband met de aansluitende besloten zitting van het AB.

Adviesnota algemeen bestuur

Voorstel van het dagelijks bestuur
15 november 2024

Openbaar	**Registratienummer**	**Datum**
Ja	2024-000021	11 december 2024

Agendapunt	**Onderdeel SamenTwente**
B1	GGD

Onderwerp
Vergoeding voor kosten inzet Jeugdgezondheidszorg (JGZ) t.b.v. Oekraïense vluchtelingen

Voorstel
1. De rijksbijdrage, die de gemeenten ontvangen voor de taken van de JGZ voor Oekraïense vluchtelingen, via separate facturatie bij de gemeenten in rekening te brengen.

Inleiding
Net zoals in 2022 en 2023 zijn gemeenten, GGD-en en veiligheidsregio's ook in 2024 hard aan het werk om opvangplekken voor Oekraïense vluchtelingen te realiseren. Op het moment dat deze vluchtelingen in Nederland worden opgevangen, hebben zij recht op zorg volgens de wet Publieke Gezondheid. Voor de JGZ wordt 2024 net als in 2022 en 2023, een separate regeling opgesteld door het ministerie van VWS voor de bekostiging. Deze bekostiging zal weer via het gemeentefonds verlopen. In de decembercirculaire van 2024 van het gemeentefonds zal deze bekend worden gemaakt. In uw vergadering van 13 december 2023 zijn voor het boekjaar 2023 afspraken gemaakt over de bekostiging. Via dit voorstel wordt voorgesteld dezelfde afspraak ook voor het jaar 2024 te maken.

Beoogd effect
De wettelijke JGZ-taken voor kinderen van Oekraïense vluchtelingen uitvoeren en hiervoor dekking realiseren.

Argumenten

1.1. De gemeenten ontvangen een bijdrage vanuit het rijk voor deze taak
Door het Rijk wordt een macrobudget beschikbaar gesteld voor de wettelijke JGZ-taken voor kinderen van Oekraïense vluchtelingen. Dit macrobudget zal middels een verdeelsleutel verdeeld worden tussen de gemeenten. Dit zal definitief bekend gemaakt worden in de decembercirculaire 2024 van het gemeentefonds. Door de rijksbijdrage separaat te factureren wordt wederom gekozen voor een taakgerichte financiering. Voor deze facturatie is geen zienswijzeprocedure benodigd omdat de gemeentelijke bijdrage niet verhoogd wordt. Dit is in overeenstemming met artikel 7.1 van onze gemeenschappelijke regeling.

1.2. Alleen het JGZ-deel van de rijksbijdrage wordt in rekening gebracht.
De rijksbijdrage die de gemeenten gaan ontvangen bestaat uit 3 onderdelen, namelijk: WMO, Jeugdwet en de uitvoering van het basistakenpakket Jeugdgezondheidszorg, waaronder het RVP en het prenataal huisbezoek uit de Wet publieke gezondheid. De facturering zal enkel betrekking hebben op het JGZ-deel van de rijksbijdrage. Dit is conform voorgaande jaren.

1.3. De werkzaamheden worden al gedaan
Sinds de toestroom van Oekraïense vluchtelingen voert de JGZ extra werkzaamheden uit. Daarom is het noodzakelijk om dekking te organiseren voor deze wettelijk verplichte taken. Met dit procesvoorstel willen wij afspraken hierover maken.

Kanttekening

1.1. De exacte hoogte van de financiering is nog niet bekend
De exacte hoogte van de financiering per gemeente zal in de decembercirculaire 2024 van het gemeentefonds bekend gemaakt worden. In 2023 werd het macrobudget verdeeld over de gemeenten op basis van het gemiddelde aantal ontheemden per gemeente. Er bestaat dus een risico dat de beschikbare middelen niet voldoende zullen zijn ter dekking van de gemaakte kosten. Net zoals in 2023, wordt in de jaarstukken 2024 verantwoording afgelegd over de besteding van deze middelen.

1.2. Dit voorstel betreft enkel de taken uit de wet Publieke Gezondheid m.b.t. de jeugdgezondheidszorg.
Binnen de wet Publieke Gezondheid vallen meer taken die door de GGD uitgevoerd worden voor de Oekraïense vluchtelingen. Denk hierbij aan infectieziektebestrijding, technische hygiëne, TBC en seksuele gezondheid. Deze taken zijn in verhouding veel minder omvangrijk dan de JGZ-taken. De meerkosten die voor deze werkzaamheden worden gemaakt worden via een SPUK regeling vergoed door het Rijk. De gemeente Wierden is de coördinerende gemeente hierin voor Twente.

1.3. De financiering voor 2025 is nog onzeker
De verwachte rijksbijdrage is bestemd voor de werkzaamheden van een heel jaar. Naar verwachting zullen de werkzaamheden in 2025 nog voortgezet moeten worden. Financiering voor het jaar 2025 is op dit moment nog onzeker. Het deel van de bekostiging 2024 dat niet benut is, zal worden overgeheveld naar het boekjaar 2025. De verantwoording en inzicht in de besteding van de middelen vindt plaats via de jaarstukken 2024 en via de Bestuursrapportages in 2025.

Kosten, baten, dekking
De kosten van dit voorstel worden in de decembercirculaire 2024 van het gemeentefonds bekend gemaakt. Het bedrag dat gemeenten zullen ontvangen vanuit het Rijk, zal separaat gefactureerd worden door SamenTwente aan de 14 Twentse gemeenten.

In onderstaand overzicht zijn de kosten en de in rekening gebrachte rijksbijdrage van 2022 en 2023 te zien. Dit overzicht is ook terug te vinden in de jaarrekening 2023 van SamenTwente. Er is nog een deel van de middelen beschikbaar. Ook is te zien dat de rijksbijdrage van 2023 niet toereikend was. Tevens wordt voorzien dat vanaf 2026 de rijksbijdrage aanzienlijk lager zal worden. Dit wordt ook toegelicht in de ontwikkelingenbrief 2026.

JGZ Oekraïense Vluchtelingen	2022	2023	Totaal
Personele kosten	220	391	611
Inhuur derden	34	23	57
Totale kosten	**254**	**414**	**668**
Rijksbijdrage (via gemeentefonds	508	351	859
Resterend	**254**	**-63**	**191**

Aantal Oekraïense jeugdigen in zorg op 31 december

	2022	2023
Instroom	1.291	342
Uitstroom	324	242
In zorg	**967**	**1.067**

Communicatie
N.v.t.

Vervolg
1. Op het moment dat de decembercirculaire gepubliceerd is zullen de genoemde bedragen per gemeente via separate facturatie in rekening worden gebracht in 2024.

Bijlagen
Geen

Besluit algemeen bestuur:

[tekst]

Enschede
11-12-2024

secretaris

drs. S. Dinsbach

voorzitter

drs. C.F.M. Bruggink

Adviesnota algemeen bestuur

Voorstel van het dagelijks bestuur
15 november 2024

Openbaar	Registratienummer	Datum
Ja	2024-000021	11 december 2024

Agendapunt	Onderdeel SamenTwente
B2	Bedrijfsvoering

Onderwerp
Nota integraal risicomanagement en weerstandsvermogen

Voorstel
1. De nota “Integraal risicomanagement en weerstandsvermogen 2024-2027” vast te stellen.
2. De oude nota “Van risicomanagement tot weerstandsvermogen 2018” in te trekken.

Inleiding
Dagelijks maken we afwegingen die van invloed kunnen zijn op het realiseren van onze maatschappelijke opgaven. De omgeving waarin SamenTwente dit doet is niet altijd voorspelbaar. We krijgen te maken met onzekerheden, risico’s en kansen. Dit kan ertoe leiden dat het onzeker is of we onze doelstellingen zullen behalen. Goed risicomanagement helpt hierbij en helpt bij het nemen van onderbouwde besluiten. Deze notitie beschrijft onze visie op risicomanagement en de uitgangspunten inclusief het hieraan gerelateerde weerstandsvermogen.

Beoogd effect
Het managen van onze doelrealisatie en voldoen aan wet- en regelgeving.

Argumenten

1.1 Dit is in overeenstemming met de financiële verordening
In overeenstemming met artikel 18 van de financiële verordening 2024 bieden wij u tenminste eens in de vier jaar een nota risicomanagement ter vaststelling aan. Dit is de eerste nota risicomanagement van SamenTwente. De huidige geldende nota is de nota risicomanagement van Regio Twente uit 2018. Het vernieuwen van deze oude nota heeft langer geduurd in verband met de ontvlechting van Regio Twente per halverwege 2021 en daarna door het managen van de coronacrisis.

1.2 We beogen een doorontwikkeling met betrekking tot risicomanagement
Afgelopen jaren hebben we aan de hand van onze nota risicomanagement uit 2018 goede stappen gezet met betrekking tot financieel risicomanagement. Jaarlijks worden financiële risico’s

geïnventariseerd en voor de geaccepteerde en resterende risico's wordt weerstandsvermogen aangehouden. In de jaarstukken wordt inzichtelijk gemaakt welke financiële risico's zich hebben voorgedaan en of hiervoor ook het weerstandsvermogen is aangesproken. In de paragraaf weerstandsvermogen zijn scenario analyses opgenomen hoe onze weerstandsratio zich ontwikkelt als tegenvallers zich voordoen en daarnaast worden de overige financiële kengetallen (zoals solvabiliteit en schuldquote) in relatie tot elkaar beschouwd. Het is nu tijd om ons risicomanagement door te ontwikkelen. Dit willen we doen door risicomanagement duidelijker te relateren aan onze doelen, breder te kijken dan alleen financiële risico's en het gesprek (risicodialoog) te stimuleren.
Met het risicodialoog willen we ervoor zorgen dat op alle ambtelijke en bestuurlijke niveaus bereidheid en ruimte is om over risico's te praten. Alleen daar waar de juiste risico`s op tafel komen, kunnen de juiste maatregelen en besluiten worden genomen. Deze ambities en de weg hiernaar toe zijn uiteengezet in hoofdstuk 4 van de nota.

2.1 Deze nota is achterhaald
Met de vaststelling van de nieuwe nota dient u ook nog een besluit te nemen om de oude nota in te trekken.

Kanttekening

1.1 Er zijn ook andere keuzes te maken met betrekking tot het weerstandsvermogen
De huidige geldende lijn met betrekking tot de ratio weerstandsvermogen is dat we streven naar een weerstandsratio van 1,0 met een ondergrens van 0,8. Deze afspraak is ook in de voorliggende nota weerstandsvermogen opgenomen. Kenmerkend voor een verbonden partij zoals SamenTwente, is dat financiële resultaten bij de vaststelling van de jaarrekening worden vereffend met de deelnemers. U zou daarom ook kunnen afspreken dat de organisatie geen weerstandsvermogen aanhoudt voor het opvangen van risico's en aan het eind van het jaar het resultaat in rekening brengt bij de gemeenten. Maar dit uitgangspunt benadrukt de mogelijkheid tot afwentelen van de risico's op de gemeenten. Bovendien stimuleert dit ook niet het risicobewustzijn van de organisatie. Daarom adviseren we dit niet. U kunt ook een hoger streefratio dan 1,0 afspreken. Dit achten wij niet noodzakelijk.

Kosten, baten, dekking
Met dit voorstel zijn geen kosten gemoeid waar dekking voor benodigd is.

Communicatie
Via de P&C cyclus wordt periodiek gerapporteerd over de invulling van deze nota.

Vervolg
- Er wordt een implementatieplan uitgewerkt met de jaarlijks uit te voeren activiteiten om onze ambities uiterlijk in 2027 gerealiseerd te hebben.

Bijlagen

Nota integraal risicomanagement en weerstandsvermogen 2024-2027

Besluit algemeen bestuur:

[tekst]
Enschede
11-12-2024

secretaris

drs. S. Dinsbach

voorzitter

drs. C.F.M. Bruggink

Gezond, veilig & vitaal

Nota integraal risicomanagement en weerstandsvermogen 2024-2027

samentwente.nl

Samen Twente

1. Besluit

Het algemeen bestuur van SamenTwente

Gelet op:

- Artikel 18 van de financiële verordening SamenTwente;
- Het Besluit begroting en verantwoording provincies en gemeenten

Besluit:

- Nota integraal risicomanagement en weerstandsvermogen 2024 tot en met 2027 vast te stellen;
- De oude nota “Van risicomanagement tot weerstandsvermogen 2018” in te trekken.

Inhoudsopgave

2. Inleiding

Dagelijks maken we afwegingen die van invloed kunnen zijn op het realiseren van maatschappelijke opgaven. De omgeving waarin SamenTwente dit doet is niet altijd voorspelbaar. We krijgen te maken met onzekerheden, risico's en kansen. Dit kan ertoe leiden dat het onzeker is of we onze doelstellingen zullen behalen. Goed risicomanagement helpt hierbij en helpt bij het nemen van onderbouwde besluiten. Risicomanagement zorgt er niet alleen voor dat risico's duidelijk worden, maar zorgt er vooral voor dat er maatregelen getroffen worden om risico's te beheersen.

Doel van deze notitie

Deze notitie beschrijft de uitgangspunten voor het risicomanagement bij SamenTwente en het hieraan gerelateerde weerstandsvermogen. Deze notitie biedt handvatten voor onze organisatie die helpend zijn voor zowel ons bestuur als de ambtelijke organisatie als het gaat om het managen en beheersen van risico's. Daarnaast zijn wij als gemeenschappelijke regeling volgens het Besluit begroting en verantwoording (BBV) wettelijk verplicht om risico's te inventariseren die van belang kunnen zijn voor onze financiële positie. Om de financiële consequenties van risico's op te kunnen vangen wordt weerstandsvermogen aangehouden. Dit zijn middelen die een buffer vormen om de financiële effecten van risico's op te vangen.

Kanttekeningen

Is risicomanagement dé oplossing voor het voorkomen van incidenten? Het antwoord is: nee. We kunnen namelijk nooit alle risico's in kaart brengen die zich in een bepaalde periode zouden kunnen voordoen. Simpelweg omdat risicomanagement geen exacte wetenschap is en bovendien zou dit ook niet doelmatig zijn. Risicomanagement vergroot wel de kans op succes, draagt bij aan de bewustwording van het werken met risico's en helpt onze organisatie om meer weloverwogen keuzes te maken.

Hebben risico's alleen een negatief effect? Ook hierop is het antwoord: Nee. Wanneer we in dit document spreken over risico`s dan hebben we het ook over kansen. Kansen die gezien worden wanneer we het hebben over het realiseren van onze doelstellingen. Risicomanagement geeft dus niet alleen inzicht in de risico`s, maar ook in de kansen.

2.1 Kaderstelling

Naast onze interne motivatie dat risicomanagement en afspraken hierover helpen bij het realiseren van doelstellingen, is er ook sprake van wet- en regelgeving die ons verplicht om hierover afspraken te maken.

Wettelijk kader

Het wettelijk kader voor dit document ligt besloten in BBV. Het BBV bevat voorschriften voor de inrichting van de begroting en de jaarstukken. Eén van de verplichtingen is het opnemen paragraaf weerstandsvermogen en risicobeheersing. Met het vaststellen van deze nota wordt het beleid voor de komende periode vastgelegd. Daarnaast zijn er verplichtingen gesteld vanuit de Baseline Informatiebeveiliging Overheid (BIO) en de NEN-7510 als het gaat om cyberrisico's en informatiebeveiliging en privacy risico's.

Provinciaal toezichtkader

De provincie Overijssel houdt toezicht op SamenTwente als gemeenschappelijke regeling. In het financieel toezichtkader voor gemeenschappelijke regelingen is opgenomen dat de provincie toetst of SamenTwente inzicht geeft in de risico's.

Financiële verordening SamenTwente
Met de financiële verordening stelt het algemeen bestuur op hoofdlijnen de financiële spelregels vast. In artikel 18 van onze financiële verordening 2024 is opgenomen dat het dagelijks bestuur tenminste eens in de vier jaar een nota risicomanagement ter vaststelling aanbiedt aan het algemeen bestuur.

2.2 Leeswijzer

De notitie begint met een managementsamenvatting waarin de belangrijkste uitgangspunten zijn opgenomen. In de navolgende hoofdstukken worden deze uitgangspunten uitgeschreven. Vervolgens wordt toegelicht hoe het risicomanagement op basis van deze uitgangspunten in de praktijk zijn uitwerking krijgt, welke aandachtspunten er zijn en welke rollen en verantwoordelijkheden bij risicomanagement horen. Deze notitie wordt afgesloten met een beschrijving van het weerstandsvermogen.

3. Managementsamenvatting

Het is belangrijk om periodiek de wijze waarop risicomanagement is ingericht tegen het licht te houden om te verbeteren en te optimaliseren. Daarnaast zijn er hiervoor ook aanleidingen vanuit de externe omgeving, zoals bijvoorbeeld het 'Besluit begroting en verantwoording' en diverse voor ons (aankomende) verplichte normen, zoals de BIO, NEN7510, NIS2, ISO 9001 en HKZ (Harmonisatie Kwaliteitsbeoordeling in de Zorgsector).

Afgezien van de externe invloeden, zien we zelf het belang groter worden voor effectief risicomanagement om onze doelstellingen te kunnen blijven behalen. Met risicomanagement willen we niet alleen ervoor zorgen dat de organisatie voldoet aan wettelijke verplichtingen, maar vooral ervoor zorgen dat effectief omgegaan kan worden met steeds veranderende en groeiende (cyber)dreigingen en uitdagingen die onze doelrealisatie in de weg kunnen staan.

Om ervoor te zorgen dat we binnen de gehele organisatie werken met een duidelijk en eenduidig kader voor risicomanagement, gebruiken we de NEN-ISO 31000 als handvat. Deze risicomanagementstandaard kan ons ondersteunen in het behalen van onze ambities op het gebied van risicomanagement, deze zijn:

- Doelgebonden: risicomanagement voegt directe waarde toe;
- Risicodialoog is prioriteit: het gaat niet om actueel houden van lijstjes;
- Eenduidig kader: uniformiteit werkwijze binnen de gehele organisatie;
- Integraal: risicomanagement doen we waar dat waarde toevoegt;
- Integraal: de juiste disciplines aan tafel;
- Integraal: aandacht voor strategisch risicomanagement en operationeel risicomanagement;

Voor het toepassen van risicomanagement is het van belang dat de processen van de organisatie waar nodig voldoende zijn beschreven en dat de rol van proceseigenaar én andere rollen voor het risicomanagement binnen de organisatie goed worden neergezet. Om het risicomanagement doelgebonden te maken en niet los te laten staan van de processen gaan we ook een applicatie gebruiken. Deze applicatie moet bijvoorbeeld een koppeling maken tussen doelen, risico's en maatregelen. Hiermee voorkomen we ook dat er op verschillende manieren en op verschillende locaties risicoregisters worden bijgehouden. Dit helpt bij het samen integraal werken aan doelrealisatie en daarmee dus ook aan risicomanagement (managen van onze doelen).

4. Onze ambitie op het gebied van integraal risicomanagement

Waarom (nu) belangrijk?
Risicomanagement is belangrijk omdat wij daardoor tijdig kunnen anticiperen op eventuele onverwachte invloeden op het kunnen behalen van onze doelstellingen en het uitvoeren van onze zorg- en dienstverlening. We merken dat risicomanagement steeds belangrijker wordt. Vanuit wet- en regelgeving moeten wij als overheidsorganisatie steeds meer aantonen dat we in control zijn als het gaat om risico's. Zie als voorbeeld de toenemende (nationale en internationale) eisen rondom informatiebeveiliging, -management en privacy maar ook regelgeving over Arbo en de veiligheid van medewerkers en de rechtmatigheidsverantwoording. Dit vergt voor risicomanagement een bredere blik dan alleen een financiële.

Waar staan we nu?
Risicomanagement kan op vele verschillende manieren ingericht worden. Om een beeld te vormen van ons huidige niveau gebruiken we een volwassenheidsmodel (zie figuur 1) dat uitgaat van 4 niveaus van risicomanagement. Op dit moment is ons risicomanagement ingericht op het voldoen wat ervanuit wet- en regelgeving van ons gevraagd wordt (niveau 2). Het is erg financieel gedreven met als focus, het opstellen van de risicoparagraaf in de begroting en de jaarstukken. De koppeling met doelrealisatie kan versterkt worden. Zonder een goede koppeling met doelrealisatie is het moeilijk om risicomanagement te laten leven in de organisatie. Risicomanagement is weinig succesvol als de reden voor het uitvoeren hiervan gelegen is in het voldoen aan de wettelijke voorschriften. Volgens ons is een interne motivatie de beste drijfveer.

Figuur 1 Risico-volwassenheidsmodel NARIS

Onze ambitie
De focus ligt de komende jaren (2024-2027) op het door ontwikkelen en verder professionaliseren van risicomanagement naar het niveau van "Proactief". Dit willen we bereiken door:

1. **Doelgericht, Integraal en uniform risicomanagement**
   Om het niveau van "Proactief" te bereiken is onze ambitie om risicomanagement integraal en zoveel als mogelijk uniform binnen de organisatie toe te passen. Met *integraal* verstaan we het breed invullen van risicomanagement (niet alleen financieel). We realiseren ons dat risicomanagement een bredere focus heeft dan enkel financieel. Daarom is het van belang om

ook aandacht te hebben voor niet-financiële risico's zoals imago, proces, en bestuurlijke risico's/aansprakelijkheid. Managers zijn verantwoordelijk voor risicomanagement in hun werkveld. Om met deze brede bril naar risico's te kunnen kijken, zorgen we ervoor dat risico's identificeren een proces is waarbij meerdere disciplines bij betrokken zijn.
Risicomanagement is geen afzonderlijke activiteit maar maakt integraal onderdeel uit van alle processen. We stimuleren het risicobewustzijn en voorkomen dat afdelingen op verschillende wijze met verschillende uitgangspunten voor risicomanagement werken. Het rekening houden met risico`s en kansen willen we terugzien in het dagelijkse denken en handelen van alle medewerkers. Daarbij leggen we een duidelijke koppeling tussen doelrealisatie en risicomanagement. Waarbij we op strategisch niveau vooral kijken naar het behalen van doelstellingen uit het vierjarige strategische programma en de programmabegroting. Op het operationele niveau kijken we naar de door vertaalde doelstellingen in de (team) jaarplannen en de processen. Bij beide gaat het om tijdig anticiperen op onverwachte invloeden die effect hebben op onze doelstellingen.
Het gebruiken van dezelfde werkwijze en uitgangspunten maakt het mogelijk om het strategische niveau met het operationele niveau te koppelen en te spreken van doelgericht, integraal en uniform risicomanagement.

2. **Dialoog stimuleren**
   Het goede gesprek over risico's en risicobereidheid is de basis van ons risicomanagement. We moeten ervoor zorgen dat op alle ambtelijke en bestuurlijke niveaus bereidheid en ruimte is om over risico's te praten. Het gaat om het ontwikkelen van een gesprekscyclus waarbij het draait om bewustwording en het voeren van een open gesprek over risico's (risicodialoog). Een goed risicodialoog is wat ons betreft een gesprek over expliciet, realistisch en gestructureerd omgaan met onzekerheden (risico's en kansen) waarbij alle deelnemers aan het gesprek vrijmoedig spreken en openhartig luisteren[1]. Bij de uitvoering van het risicodialoog stellen we drie vragen centraal:
   - Wat is ons doel?
   - Wat is daarbij onzeker (wat zijn de risico's en kansen)?
   - Wat staat ons vanuit onze risicobereidheid te doen?

Met de hierboven uiteengezette twee punten is onze ambitie dat risicomanagement meer gaat leven en meer wordt dan enkel een financieel technische exercitie eens per jaar voor de paragraaf weerstandsvermogen.

[1] Van Staveren, 2023

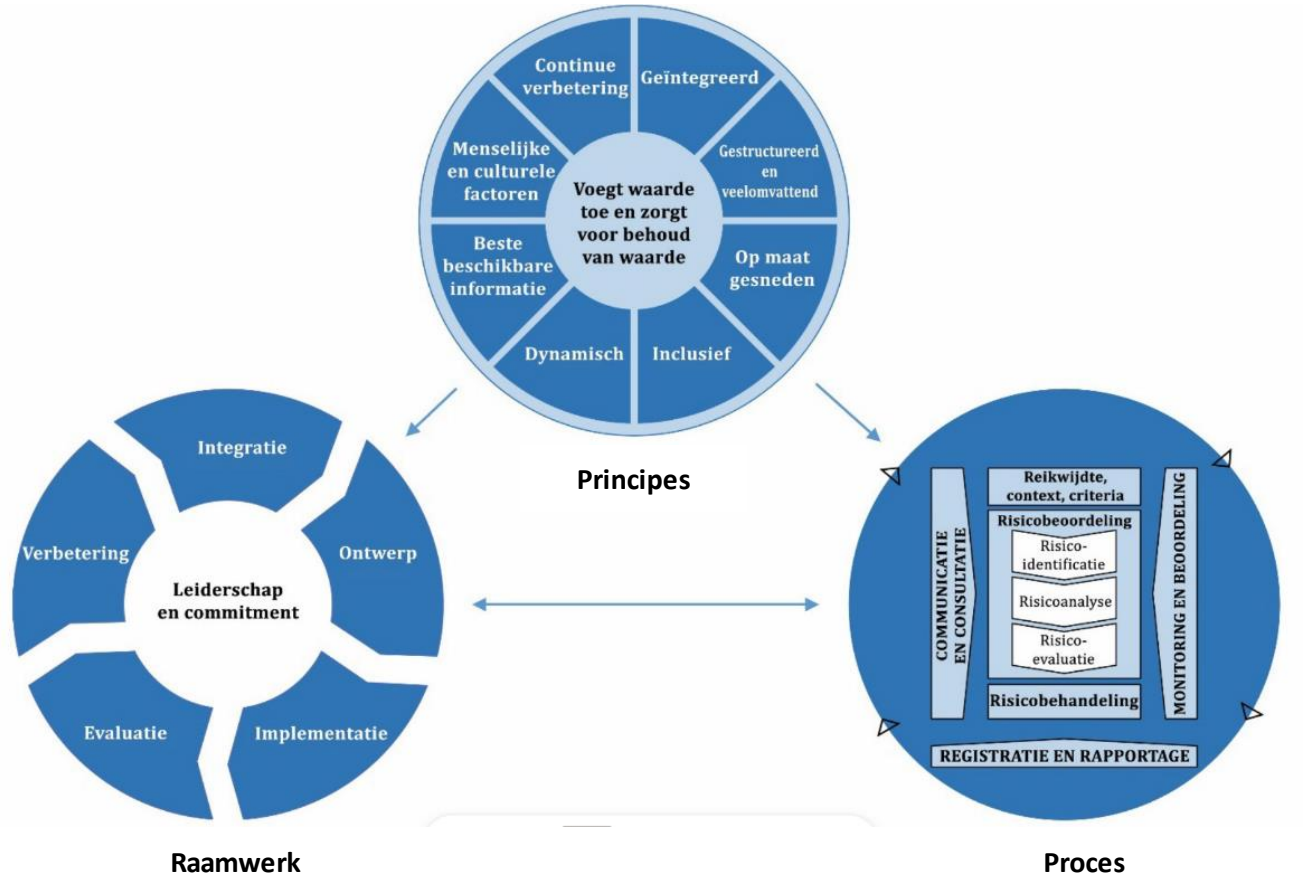
5. Integraal risicomanagement volgens de NEN-ISO 31000

Om het risicomanagement integraal bij SamenTwente in te kunnen richten is een raamwerk nodig. Hiervoor hebben wij gekozen voor de internationale standaard NEN-ISO 31000.

Waarom de NEN-ISO 31000

De NEN-ISO 31000 is een internationale richtlijn voor risicomanagement. Het heeft als doel om de kans op het behalen van doelstellingen te vergroten. Het voorziet daarvoor in een werkwijze op zowel strategisch als operationeel niveau voor de identificatie van kansen en bedreigingen in combinatie met de behandeling hiervan.

Deze richtlijn biedt een eenduidig raamwerk, taal en werkwijze voor de verschillende vormen van risicomanagement binnen een organisatie. De NEN-ISO 31000 is een vrij toe te passen richtlijn en kan door de organisatie zelf op maat worden gemaakt. Hierdoor wordt voorkomen dat risicomanagement naast de reguliere bedrijfsvoering komt te staan en gezien wordt als een ongewenste bureaucratische aanvulling op het dagelijkse werk. Bij diverse overheden wordt NEN-ISO 31000 dan ook veelvuldig toegepast. Wij zien de NEN-ISO 31000 als ondersteunend aan onze in hoofdstuk 4 verwoorde ambities. In onderstaande figuur is de NEN-ISO 31000 weergegeven. Deze norm zet de principes, het raamwerk en het proces van integraal risicomanagement uiteen.



Figuur 2 NEN- ISO 31000

Principes voor effectief risicomanagement (hoofdstuk 6.1)
De NEN-ISO 31000 geeft principes (te zien als randvoorwaarden) die ingevuld moeten zijn en continu gestimuleerd moeten worden om het risicomanagement binnen organisatie effectief te houden. De principes stellen de organisatie in staat om de effecten van onzekerheden op haar doelstellingen op goede en gestructureerde wijze te managen. Principes zijn richtinggevend voor de opzet van doelmatig en doeltreffend risicomanagement.

Raamwerk voor risicomanagement (hoofdstuk 6.2)
Het doel van het raamwerk voor risicomanagement is om de organisatie te helpen om risicomanagement in belangrijke activiteiten en functies te integreren. Zodat het rekening houden met risico`s en kansen en alle relevante processen terug te vinden is. Doeltreffendheid van risicomanagement hangt hiervan af. Dit vereist draagvlak vanuit belanghebbenden en leiderschap commitment van het management en het bestuur. Het ontwikkelen van het raamwerk omvat het integreren, ontwerpen, implementeren, evalueren en verbeteren van risicomanagement in de hele organisatie. Waarbij de verschillende componenten samenwerken en op maat zijn gemaakt voor het specifieke proces (de activiteit). Zo krijgt het risicomanagement voor projectmanagement bijvoorbeeld een andere invulling dan het risicomanagement voor uitvoerende zorgprocessen (zoals het zetten van vaccinaties).

Het proces van risico`s identificeren t/m behandeling (hoofdstuk 6.3)
Rekening houden met risico`s en kansen in de processen impliceert dat je op een bepaald moment in een proces nadenkt over risico's en kansen en er vervolgens de juiste maatregelen bij bepaald. Voor het borgen van de uniformiteit biedt de NEN-ISO 3100 enkele vaste stappen. Een risicomanagementproces start altijd met het vaststellen van reikwijdte, context en criteria. In het proces is communicatie en consultatie met belanghebbenden verankerd en wordt het monitoren en beoordelen van risico's geborgd. De NEN-ISO 31000 is geen "one size fits all". Er is ruimte voor proportionaliteit. Dat wil zeggen dat organisatieonderdelen en/of projecten met een hoog risicoprofiel en groot belang voor het functioneren van onze organisatie, het risicomanagement zwaarder kunnen aanzetten dan waar dat minder het geval is.

In de volgende hoofdstukken wordt aangegeven hoe de NEN-ISO 31000 wordt toegepast bij SamenTwente.

6. Toepassing bij SamenTwente

In dit hoofdstuk worden de uitgangspunten beschreven zoals wij dit gaan toepassen bij het ontwerpen, implementeren en evalueren van het risicomanagement van SamenTwente.

6.1 Toepassing principes voor effectief risicomanagement

De principes (te beschouwen als voorwaarden) vormen de basis voor het managen van risico`s en kansen. De mate van en de invulling van de principes kan per organisatie verschillen en daarom dienen de principes ook op maat te worden gemaakt. Dit doen we op het moment dat we concreet processen gaan beschrijven of bestaande processen gaan aanpassen om het risicomanagement proces (de stappen) te integreren. Een voorbeeld hiervan is dat het risicomanagement dynamisch moet zijn. In praktijk betekent dat wij niet alleen op vaste geplande momenten moeten kijken naar risico`s. Maar dat wij dat ook doen wanneer de externe of interne omgeving van de organisatie verandert. In bijlage 3 is beschreven welke principes vanuit de ISO 31000 worden gehanteerd en hoe wij deze gaan toepassen bij het ontwerpen, implementeren en evalueren van het risicomanagement van SamenTwente.

Risicomanagement en de processen van SamenTwente

Wanneer je als organisatie binnen de processen rekening wilt houden met risico`s en kansen, dan is het van belang inzichtelijk te hebben hoe de processen verlopen. Hiervoor is het van belang dat we als organisatie heldere en actuele procesbeschrijvingen hanteren en beheren in het kwaliteitsmanagementsysteem. We streven naar actuele procesbeschrijvingen, maar ook geven we bijhorende proceseigenaren een duidelijke taak- en verantwoordelijkheid bij het tijdig rekening houden met risico`s en kansen in zijn of haar proces.

Risico-register

Om zicht en grip te houden op je risico`s is het van belang dat deze risico`s ergens op een eenduidige wijze zijn vastgelegd. Dit voorkomt het zoeken naar (mogelijk verouderde) Excel documenten of andersoortige documenten waarin de risico`s staan.
Hiervoor gaan we een toegankelijke applicatie hanteren die ons gaat helpen bij het actueel houden van risico`s en bijhorende maatregelen. Bovendien wordt het hierdoor mogelijk om risico's te aggregeren en om risico`s rechtstreeks te koppelen aan processen.
Bij aggregeren gaat het bijvoorbeeld om het meenemen van de operationele risico`s bij de beoordelingen op het strategische niveau.
Bij het koppelen aan processen gaat het om de maatregelen die worden bedacht. Die kunnen dan gelijk landen in de juiste processen om daar verbeteringen te realiseren (de risico barrière). Maar ook wordt het dan mogelijk om bij het evalueren (het actualiseren) van procesbeschrijvingen de al bekende risico`s mee te nemen.

6.2 Toepassing effectief raamwerk voor risicomanagement

Het proces gaan we zoveel als mogelijk integreren binnen de bestaande processen van de organisatie. Hierbij maken we onderscheid in strategisch en operationeel risicomanagement.

Strategisch risicomanagement

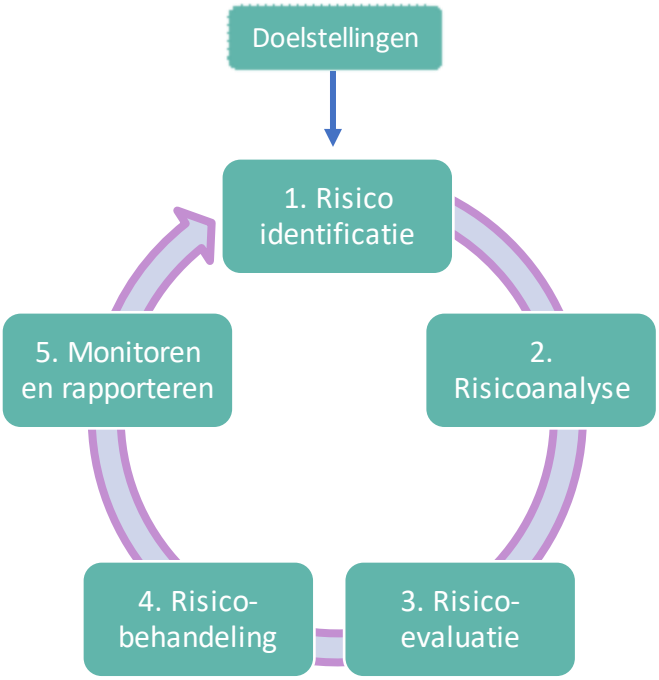
Strategisch risicomanagement gaat over het managen van risico's gerelateerd aan onze strategie en lange termijn doelstellingen. Bij het nastreven van de gestelde doelen kunnen risico's aanwezig zijn, daarom moet nagedacht worden over welke bereidheid er is om risico te lopen. Dit noemen we risicobereidheid. Risicobereidheid (of risk appetite) hangt nauw samen met organisatie strategie en is

daarmee onderdeel van strategisch risicomanagement. De risicobereidheid is de mate waarin een organisatie bewust risico's accepteert. Denk bijvoorbeeld aan informatiebeveiliging, 100% foutloos werken kan niet. Maar tegelijkertijd is belangrijk om te realiseren dat informatiebeveiligingsrisico's ook onderdeel zijn van het strategisch risicomanagement.
Het vaststellen van je risicobereidheid kan helpen bij het bepalen van de prioriteiten. Het bepalen van de risicobereidheid is taak van directie en management. Top down. Hierbij is het belangrijk om een terugkerende dialoog organiseren. Ter ondersteuning van de dialoog is volgens ons een risicomatrix (zie hoofdstuk 6.3.2) een goed instrument. Hiermee kan directie en management duidelijkheid verschaffen over de 10 tot 15 belangrijkste strategische risico's die de prestatie van onze organisatie beïnvloeden. Strategische risico's zijn risico's die inherent zijn aan het ontwikkelen en uitvoeren van beleid en zijn daarom ook niet per definitie altijd ongewenst.
Zoals u in de inleiding heeft kunnen lezen wordt SamenTwente vanuit diverse wet- en regelgeving (BBV, BIO, NEN7510, NIS2 etc.) verplicht om risico's te inventariseren die van belang kunnen zijn voor onze financiële positie. Om de financiële consequenties van risico's op te kunnen vangen wordt weerstandsvermogen aangehouden. Ook dit is onderdeel van strategisch risicomanagement van SamenTwente.

Operationeel risicomanagement
Operationele risico's zijn veelal interne risico's, voortkomend uit de organisatie, die beheersbaar zijn en vermeden of zoveel als mogelijk opgelost moeten worden. Voorbeelden zijn risico's van onrechtmatig handen, fouten in (geautomatiseerde) processen en ongeautoriseerde toegang. Operationele risico's kunnen risico's zijn die voortvloeien uit wet- en regelgeving (compliancy) maar het gaat ook om risico's bij de uitvoering van onze taken zoals het uitvoeren van vaccinaties. Hierbij gaat het om het treffen van beheersmaatregelen en ervoor te zorgen dat er sprake van een continu proces van controleren en evalueren. Ook in het operationele risicomanagement is er sprake van risicobereidheid. Het gesprek hierover ligt dan op het niveau van teamleiders in afstemming met het management.

6.3 Het proces van risico's identificeren t/m rapporteren

Het risicomanagement proces, op strategisch en operationeel niveau, beschrijft de stappen van risico identificatie, analyse en evaluatie.



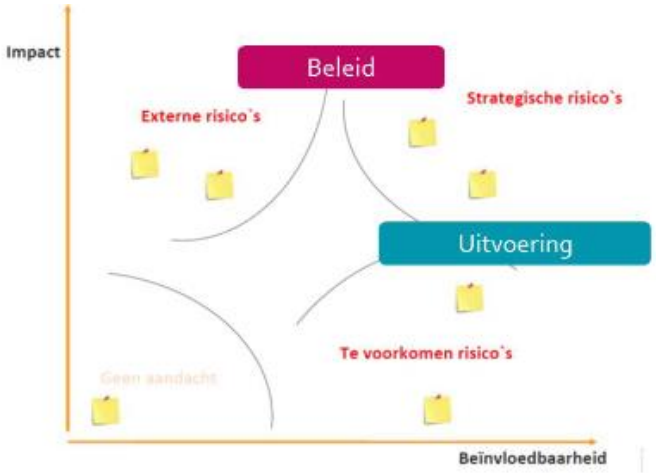
Dit risicomanagement proces gaan we toepassen waar dit waarde toevoegt aan het beter kunnen realiseren van doelstellingen. Op het strategische niveau zien we dat terug in de planning- en control cyclus en voor het operationeel niveau valt bijvoorbeeld te denken aan:

- Realisatie van jaar- en teamplannen.
- Projectmanagement

Op de volgende pagina`s wordt het risicomanagement proces toegelicht.

6.3.1 Risico-identificatie

Bij de identificatie van risico`s onderscheiden we operationele risico's (bijvoorbeeld fouten in geautomatiseerde processen), strategische risico's (bijvoorbeeld risico's die invloed hebben op de gestelde doelen in de programmabegroting) en externe risico's. Externe risico's worden gekenmerkt doordat de oorzaak van het risico zich buiten ons invloedsfeer bevindt, zoals een pandemie. Bij dit type risico moet wel een vertaalslag plaatsvinden naar de concrete risico's voor onze organisatie (bijvoorbeeld het risico dat extra taken uitgevoerd moeten worden door een pandemie, het risico dat er extra personeel ingezet moet worden dan begroot en/of het risico op tegenvallende opbrengsten). Zie bijlage 2 voor een verdere uitwerking van de soorten en type risico's. Het typeren van risico's helpt bij het omgaan van risico's. Hieronder wordt schematisch per soort risico weergegeven of de mate van impact en beïnvloedbaarheid van het risico laag of hoog is. Hieruit valt op te maken dat bij het opstellen van beleid rekening gehouden moet worden met de externe en strategische risico's en dat bij de uitvoering door de organisatie de focus hoofdzakelijk ligt op strategische en te voorkomen/operationele risico's.



Figuur 3 Soorten risico's naar impact en beïnvloedbaarheid

6.3.2 Risicoanalyses

We vinden het onwenselijk om te sturen op alle risico's. Dit is niet doeltreffend risicomanagement. Bij de risicoanalyse gaat het er om ordening in de lijst met risico's aan te brengen, zodat de meeste tijd en energie gestoken kan worden in de beheersing van en sturing op risico's die de grootste impact kunnen hebben op onze doelstellingen. Uit de fase van risico-inventarisatie volgt een lijst met risico's die onderling erg verschillen. Om een ordening hieraan te brengen bepalen we:

a) de geschatte omvang van het risico (impact op doelstelling);
b) de waarschijnlijk dat het risico zich voordoet (kans).

Risicomatrix

Bij SamenTwente gaan we uit van deze risicomatrix:

Kans van optreden	Zeer waarschijnlijk	5					
	Waarschijnlijk	4					
	Is wel eens voorgekomen	3					
	Onwaarschijnlijk	2					
	Zeer onwaarschijnlijk	1					
			1	2	3	4	5
Impact op doelstelling			Zeer klein	Klein	Gemiddeld	Groot	Zeer groot

Nadat we de risico's hebben geïdentificeerd kan de kans en impact worden bepaald. Als hulpmiddel wordt de kans en impact ingedeeld in klassen van 1 t/m 5. Door het vermenigvuldigen van de scores op geschatte kans en impact, kan per risico een risicoscore worden uitgerekend. Bijvoorbeeld: kans klasse is 4 en de impact klasse is 3, dan is de risicoscore 4 x 3 = 12.

Voor financiële risico's kan een geschat bedrag bepaald worden voor de impact. De risicoscore is een maatstaf voor de potentiële impact van het risico. Op basis van deze risicoscores kunnen risico's worden gerangschikt. Hierbij geldt dat, hoe hoger de risicoscore:

- hoe groter de potentiële impact;
- hoe hogere prioriteit de aanpak van het risico heeft.

In de volgende paragrafen wordt toegelicht hoe de matrix is opgebouwd.

Kans klassen

We maken ook een inschatting van de waarschijnlijkheid dat het risico zich daadwerkelijk voor kan doen.

Klasse	Mate van waarschijnlijkheid	Percentage
1.	Zeer onwaarschijnlijk	10%
2.	Onwaarschijnlijk	30%
3.	Is wel eens voorgekomen	50%
4.	Waarschijnlijk	70%
5.	Zeer waarschijnlijk	90%

Toelichting op de klassen:

1. Zeer onwaarschijnlijk hanteren we voor risico's waarvan het zeer onwaarschijnlijk is dat het risico zich voordoet. Denk hierbij bijvoorbeeld aan risico's die op basis van ervaringscijfers slechts één keer in de 10 jaar voordoen.
2. Onwaarschijnlijk we voor risico's waarvan het niet zo waarschijnlijk is dat het zich gaat voordoen. Bijvoorbeeld aan risico's die op basis van ervaringscijfers één keer in de 5 jaar voordoet.
3. Is wel eens voorgekomen hanteren we voor risico's die nog beide kanten op kunnen. Het kan zijn dat die zich voor doet, het kan ook zijn van niet. Denk hierbij aan risico's die op basis van ervaringscijfers slechts één keer in de 2 jaar optreden.
4. Waarschijnlijk hanteren we voor risico's waarvan het waarschijnlijk is dat die zich het komend jaar voordoet. Dit zijn risico's die op basis van ervaringscijfers jaarlijks voordoen.
5. Zeer waarschijnlijk hanteren we voor risico's waarvan het zeer waarschijnlijk is dat die optreden. Dit zijn risico's die op basis van ervaringscijfers meerdere keren per jaar voordoen

Impact klassen

a. Impact klasse voor niet-financiële risico's

Het bepalen van de omvang bij niet-financiële risico's is anders dan bij risico's met financiële gevolgen. De gevolgschade kan namelijk niet uitgedrukt worden in geld. Om toch de impact in risicoklassen hiervan te kunnen bepalen wordt gebruikt gemaakt van onderstaande risicoklassen. Onderstaande indelingen bieden handvatten voor de focus in sturing en beheersing van risico's met niet financiële impact.

Klasse	Impact
1.	Zeer klein
2.	Klein
3.	Gemiddeld
4.	Groot
5.	Zeer groot

b. Impact klasse voor financiële risico's

Bij het bepalen van de geschatte financiële omvang gaan we uit van een situatie dat het risico zich daadwerkelijk voordoet. Vanuit de gedachte "als het risico zich voordoet, dan…" maken we een inschatting van het bedrag dat naar alle waarschijnlijkheid SamenTwente kwijt is als het risico zich voordoet.

Klasse	Bandbreedte in €	Risico bedrag in €
1.	25.000 < > 50.000	37.500
2.	50.000 < > 100.000	75.000
3.	100.000 < > 200.000	150.000
4.	200.000 < > 500.000	350.000
5.	> 500.000	P.M.

Er zijn risico's die verwaarloosbaar zijn omdat de kans dat ze zich voordoen zo klein is of de financiële gevolgen zo gering, dat het vanuit de doelmatigheidsoptiek niet aan te bevelen is om daar tegen maatregelen te treffen. Het is daarom wenselijk een ondergrens vast te stellen. SamenTwente hanteert voor het kwantificeren van de risico's een ondergrens van € 25.000 als uitgangspunt.

De risico's met een financieel risico onder deze grens kunnen wel benoemd worden, maar worden niet meegerekend. Indien de impact van een bepaald risico in klasse 5 valt en dus groter is dan € 500.000, dient voor dat risico ook het maximale verwachte gevolg in euro's aan te worden gegeven. Deze situatie zou zich vooral voor kunnen doen bij majeure projecten. Het maximale gevolg in euro's fungeert vervolgens als risicobedrag voor impactklasse 5.

Voor risico's met structurele gevolgen tellen alleen de verwachte gevolgen in de eerste drie jaar mee voor een dalend percentage (1e jaar 100%, 2e jaar 50% en 3e jaar 25% = totaal € 175%). Volgens deze aflopende lijn moeten de gevolgen van het risico na jaar 3 zijn opgevangen.

6.3.3 Risico-evaluatie

Nadat de risico's zijn geïdentificeerd en geanalyseerd komen we bij de risico-evaluatie fase. Het doel van deze derde stap in het risicomanagement proces is het ondersteunen van besluiten. Hierbij gaat het om sturing op en beheersing van risico's door beheersmaatregelen te treffen. Dit is een maatregel die de kans van het optreden of de gevolgen van het optreden van een risico verkleint. Hierbij is het van belang dat de maatregelen proportioneel zijn. Dit houdt in dat de kosten van de maatregel in verhouding staan tot de vermindering van de kans of de gevolgen en dat er niet onnodig veel maatregelen voor één risico genomen worden. Er zijn 4 mogelijkheden om te bepalen wat er met het risico moet gebeuren:

1. vermijden van het risico door te besluiten de activiteit waardoor het risico wordt veroorzaakt te stoppen of door doelstelling aan te passen;
2. verminderen van de impact van het risico door ofwel de omvang van het risico terug te brengen (door bijvoorbeeld fasering) ofwel de kans/waarschijnlijkheid van optreden terug te brengen;
3. overdragen/delen van het risico door bijvoorbeeld het beleid (en/of het proces) wat het risico met zich brengt uit te laten voeren door een andere partij. Hierbij kan gedacht worden aan garanties, derden aansprakelijk stellen, contracten en verzekeringen;
4. als geen van de bovenstaande opties (vermijden, verminderen, overdragen) mogelijk of wenselijk is, kan gekozen worden om het risico te accepteren. Dit kan ook het geval zijn bij

externe risico's waarop we niet kunnen sturen. De keuze om een risico te accepteren wordt bewust gemaakt. We schatten de kans en het mogelijk financieel gevolg van een geaccepteerde risico in. Deze financiële impact wordt vervolgens opgenomen in ons risicoprofiel en wordt door het weerstandsvermogen gedekt (hoofdstuk 9).

Bruto en netto risico's

Vermijden elimineert een risico. Verminderen en overdragen verlagen de netto omvang van een risico:

Bruto verwachte omvang risico =	Verwachte gevolgschade van risico	
	Reductie risico door beheersmaatregelen	-/-
	Compensatie van derden / verhaal op derden	-/-
Netto verwachte omvang =	Nog te dekken gevolg van een risico (weerstandsvermogen)	

6.3.4 Risico-behandeling

Maatregelen voor de reductie van de impact van risico's liggen zowel op het strategische als op het operationele vlak. Het gaat hierbij niet alleen om het kiezen van maatregelen en het implementeren ervan, maar ook om het bewaken en controleren dat de gekozen maatregelen effect hebben en het zo nodig bijsturen hierop. Eerste aandachtspunt bij risicomanagement zijn de risico's die het hoogste scoren in de risicokaart (tabel 1). Ook belangrijk is om aandacht te hebben voor risico's die zelden voor komen maar als ze zich voordoen, dan is de impact enorm. Deze risico's worden ook wel zwarte zwanen genoemd. Onze organisatie heeft dit meegemaakt met de uitbraak van het coronavirus. Het beheersen van dit soort risico's is echter complex. Een beheersmaatregel kan zijn het hebben van een continuiteitsplan en zorgen dat je voldoende weerbaar bent door het organiseren van een financiële buffer.

6.3.5 Monitoren en rapporteren

Planning & control cyclus

Risicomanagement is een lerend proces. Het gaat om steeds beter omgaan met onzekerheden die onze doelen kunnen beïnvloeden. Risicomanagement past daarom goed binnen de bestaande planning & control cyclus van SamenTwente. In deze cyclus draait het om het maken van strategische plannen en het beheerst uitvoeren daarvan. Dit vraagt om sturing op doelen die we willen realiseren en verantwoording afleggen over het al dan niet realiseren daarvan. Daar hoort bij dat je bewust omgaat met onzekerheden, kansen en risico's en daar regelmatig het gesprek over voert.

Dialoog organiseren

In onze planning & control cyclus werken we met een gesprekscyclus waarin we ook het gesprek over risico's terug willen laten komen. We voeren jaarlijks bij het opstellen van onze doelen het gesprek over risico's, kansen en beheersmaatregelen. Vanaf 2024 werken we met een viermaands-cyclus. Elke vier-maanden voeren we zowel op het management- en teamleider niveau als op bestuurlijk niveau gesprekken over de realisatie van doelen, prestaties, beheersing van processen en van budgetten. Het gesprek over kansen en risico's wordt bij SamenTwente ook hier vormgegeven. We zijn deze gesprekken op dit moment steeds beter aan het structureren. Hierin leren we continue.

Rapporteren

In de paragraaf Weerstandsvermogen en risicobeheersing van de programmabegroting en jaarstukken brengen we tenminste de grootste risico's (top 10) periodiek in beeld. In het volgende hoofdstuk gaan we dieper in op het onderwerp weerstandsvermogen.

Bestuursvoorstellen
Het dagelijks bestuur heeft de opdracht van het algemeen bestuur om de gestelde doelen in de programmabegroting te behalen. Het dagelijks bestuur staat bij de uitvoering van de doelen soms voor complexe keuzes. Voor het maken van een bewuste keuze is het hebben van een goed beeld van de argumenten voor en tegen, met de hieraan gekoppelde risico`s en risicobereidheid, noodzakelijk. Het is dus van belang dat in bestuursvoorstellen de risico's duidelijk worden benoemd en de afwegingen die hierbij zijn gemaakt of worden voorgesteld. Hierbij houden we rekening met de in bijlage 2 uiteengezette soorten risico's.

7. Belangrijke aandachtspunten bij risicomanagement

Sinds onze vorige beleidsnota "Van risicomanagement tot reserves en voorzieningen" uit 2018 is veel ervaring opgedaan met risicomanagement. Ook door het uitvoeren van (complexe) projecten en het evalueren hiervan hebben we lessen geleerd en aandachtspunten opgedaan die belangrijk zijn bij risicomanagement.

Verschillende vormen van risicobeheersing en tegendenkkracht organiseren
Het is belangrijk om bij (complexe) projecten waarbij veel (en soms tegengestelde) belangen spelen verschillende instrumenten in te zetten om risico's zichtbaar te maken, te voorkomen of beheersbaar te houden. Hierbij is het belangrijk om vooraf maar ook gedurende het project risico's in beeld te (blijven) brengen. Bij het in beeld brengen is het van belang om aandacht te hebben voor risico's met een kleine kans maar met een grote impact. Om dit scherp in beeld te brengen organiseren wij voldoende tegendenkkracht. Deze tegendenkkracht kan bijvoorbeeld intern georganiseerd worden door bij het inventariseren van risico's (bijvoorbeeld tijdens een risicodialoog) verschillende disciplines te betrekken. Hiermee borgen we dat er vanuit verschillende invalshoeken wordt gekeken. Er kan ook externe expertise ingehuurd worden door bijvoorbeeld het laten uitvoeren van een externe juridische toets of door het laten uitvoeren van een onafhankelijke risico-inventarisatie.

Risico optimisme
Inschatting van risico's gebeurt niet altijd rationeel en daardoor bestaat de kans dat risico's onderschat worden. Dit kan bijvoorbeeld door kosten laag in te schatten en/of het tijdsbeslag om een project te realiseren onbewust wordt onderschat. Het is belangrijk om vooraf te realiseren dat deze risico optimisme kan gebeuren. Het is belangrijk om een cultuur te creëren waarbij dit bespreekbaar is en altijd helder en transparant te communiceren over de mogelijke hogere kosten en/of langere tijd die met het project kan zijn gemoeid.

Het is niet mogelijk alle risico's in te schatten en risicobeheersing is geen garantie voor succes
De realiteit is ook dat het niet mogelijk is alle risico's die SamenTwente loopt op voorhand te onderkennen. In onze complexe samenleving doen zich altijd verrassingen voor. Deze kunnen grote impact hebben. Risico's kunnen zich ook altijd op onvoorziene wijzen manifesteren in een project.

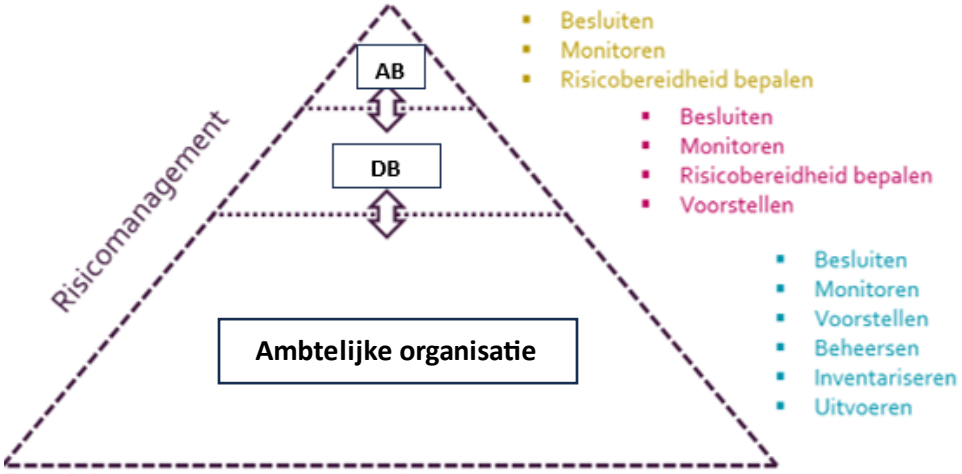
Risicoregelreflex
Wanneer een risico zich heeft voorgedaan in de vorm van een incident is meestal de reactie "dit had nooit mogen gebeuren en dus moeten we het liefst direct maatregelen treffen". Dit noemen we de risicoregelreflex. Dit reflex is soms adequaat, maar soms leidt dit ook tot een overmaat aan maatregelen die hoge kosten met zich meebrengen. Door bewust stil te staan en maatregelen goed te overwegen en incidenten te onderzoeken, kan SamenTwente goed omgaan met dit reflex.

8. Rollen en verantwoordelijkheden

Bij het ontwerpen en implementeren van risicomanagement is het van belang afspraken te maken over rollen en verantwoordelijkheden.

Hieronder is in figuur 4 schematisch weergegeven welke rollen het algemeen bestuur (AB), dagelijks bestuur (DB) en de ambtelijke organisatie hebben bij het risicomanagement binnen SamenTwente. Het algemeen bestuur en het dagelijks bestuur nemen voornamelijk besluiten waarbij risico`s worden afgewogen, bepalen de risicobereidheid en monitoren via de planning en control cyclus de grootste risico`s en het weerstandvermogen. Zij stellen de kaders waarbinnen de organisatie de risico's kan beheersen, mitigeren en/of accepteren. De ambtelijke organisatie heeft de grootste rol binnen het risicomanagement. Zij zorgt er met name voor dat het dagelijks bestuur en het algemeen bestuur risicobewuste keuzes kunnen maken. Het inventariseren, kwantificeren en beheersen ligt dan ook met name bij de organisatie. De medewerkers die verantwoordelijk zijn voor de uitvoering van doelen, projecten en processen zijn ook de risico-eigenaren van de hieraan gekoppelde risico`s

Verantwoordelijkheden bij het uitvoeren van risicomanagement:



Figuur 4 Overzicht rollen en verantwoordelijkheden

Wie	Wat
Algemeen bestuur	Vaststellen kaders risicomanagement en weerstandsvermogen
	Vaststellen paragraaf weerstandsvermogen en risicobeheersing (in de begroting)
Auditcommissie	Adviseren van het algemeen bestuur over de rechtmatigheidsverantwoording en accountantscontroles.
Dagelijks bestuur	Verantwoordelijk voor realisatie van doelen en beheersen van risico's die daarmee gemoeid zijn.
	Rapporteren aan het algemeen bestuur over de belangrijkste risico's via bestuursvoorstellen en reguliere P&C cyclus
Centraal managementteam (CMT)	Verantwoordelijk voor sturing op en beheersing van organisatie brede **strategische risico's en maatregelen.**
	Zorgdragen voor vergroten risicobewustzijn
	Rapporteren aan dagelijks bestuur over risico's via bestuursvoorstellen en via de reguliere P&C cyclus
Managers	Verantwoordelijk voor sturing op en beheersing van risico's en maatregelen op afdelingsniveau.
	Zorgdragen voor vergroten risicobewustzijn
	Doorlopen van risicomanagementproces (inventarisatie en beoordeling van **strategische risico's.**
	Rapporteren aan het CMT over **strategische risico's.**
Financieel adviseurs/ business control	Stimuleren, adviseren en begeleiden van de managers bij het doorlopen van het **strategische** risicomanagementproces
Teamleiders	Verantwoordelijk voor sturing op en beheersing van risico's en maatregelen op teamniveau.
	Zorgdragen voor vergroten risicobewustzijn van medewerkers en begeleiding van medewerkers.
	Doorlopen van risicomanagementproces (inventarisatie en beoordeling van **operationele risico's).**
Medewerkers	Doorlopen van risicomanagementproces (inventarisatie en beoordeling van **operationele risico's).**
Kwaliteitsadviseurs	Stimuleren, adviseren en begeleiden van teamleiders en medewerkers bij het **operationele** risicomanagementproces.
	Zorgdragen voor vergroten risicobewustzijn.
Medewerker Verbijzonderde interne controle / auditors	Toetsen belangrijkste risico's in processen en de opzet, bestaan en werking van de beheersmaatregelen.
Concerncontroller	Toetst de kwaliteit van de organisatie brede **strategische** risico-inventarisatie en bewaakt de weerbaarheid van de organisatie.
	Zorgdragen voor vergroten risicobewustzijn.
	Verantwoordelijk voor het organisatie brede kader voor risicomanagement en weerstandsvermogen.
Adviseur crisisbeheersing GGD Twente	Inventariseren van en advisering over risico's die tot een crisis kunnen leiden
	Zorgdragen voor vergroten van risicobewustzijn

Chief Information Security Officer (CISO)	Bewaking van informatiebeveiliging-risico's en adviseren van de organisatie hierover.
	Zorgdragen voor vergroten risicobewustzijn
Functionaris Gegevensbescherming (FG)	Bewaking van privacy-risico's en adviseren van de organisatie hierover.
	Zorgdragen voor vergroten risicobewustzijn

9. Weerstandsvermogen

We zijn volgens het BBV verplicht om aan te tonen dat onze organisatie in staat is de gevolgen van risico's op te vangen zonder dat onze beleidsuitvoering in gevaar komt. Dit doen wij aan de hand van de ratio weerstandsvermogen. Het weerstandsvermogen geeft aan in hoeverre onze organisatie in staat is (weerbaarheid) negatieve financiële consequenties van risico's zelfstandig op te vangen.

Het weerstandsvermogen bestaat uit de relatie tussen

a. de beschikbare weerstandscapaciteit, zijnde de middelen en mogelijkheden waarover onze organisatie beschikt of kan beschikken om niet begrote kosten te dekken;
b. de benodigde weerstandscapaciteit, zijnde alle risico's waarvoor geen maatregelen zijn getroffen en die impactvol kunnen zijn in relatie tot onze financiële positie.

Om het weerstandsvermogen te kunnen beoordelen, zetten we de *benodigde weerstandscapaciteit* af tegen de *beschikbare weerstandscapaciteit*. De uitkomst van deze berekening vormt de *ratio weerstandsvermogen*.

$$\text{Ratio weerstandsvermogen} = \frac{\text{Beschikbare weerstandscapaciteit /}}{\text{Benodigde weerstandscapaciteit}}$$

Beschikbare weerstandscapaciteit

Om te kunnen beoordelen of we in staat zijn om risico's op te vangen wordt in beeld gebracht welke capaciteit we hiervoor beschikbaar hebben. Hierbij maken we onderscheid in incidentele en structurele weerstandscapaciteit.

Incidentele weerstandscapaciteit

Hieronder beschouwen we de algemene reserve van SamenTwente en de beschikbare egalisatiebestemmingsreserves. Ook stille reserves (verhandelbare bezittingen die gewaardeerd zijn lager dan de verkoopwaarde) maken onderdeel uit van incidentele weerstandscapaciteit. De gedachte hierachter is dat bij verkoop van deze bezittingen winst ontstaat die eenmalig inzetbaar is om tegenvallers op te vangen. Bij SamenTwente is geen sprake van stille reserves.

Structurele weerstandscapaciteit

De structurele weerstandscapaciteit bestaat veelal uit een structurele post onvoorzien en/of uit begrotingsruimte. In overeenstemming met het besluit van het algemeen bestuur ramen wij een post onvoorzien in de begroting maar de dekking hiervan is afkomstig uit de algemene reserve. Hiermee is de dekking van post onvoorzien feitelijk niet structureel. Als de begroting (inclusief de meerjarenraming) op een positief saldo sluit dan is er sprake van begrotingsruimte. Deze ruimte zou ook ingezet kunnen worden om structurele financiële tegenvallers op te kunnen vangen. SamenTwente heeft geen structurele begrotingsruimte en daarmee dus ook geen structurele beschikbare weerstandscapaciteit.

Benodigde weerstandscapaciteit

De benodigde weerstandscapaciteit wordt bepaald door de geïdentificeerde risico's uit te drukken in euro's. Dit betreffen alle risico's waarvoor geen/onvoldoende maatregelen zijn getroffen (netto verwachte omvang). Op deze wij wijze hebben we in beeld welke weerstandscapaciteit er nodig is om de financiële impact van risico's op te vangen als deze zich voordoen.

Ratio weerstandsvermogen en norm SamenTwente
SamenTwente streeft naar voldoende weerstandsvermogen. Dit staat gelijk aan een ratio weerstandsvermogen van maximaal 1,0. Als minimale toegestane ondergrens merken we de ratio weerstandsvermogen van 0,8 aan. We kiezen voor een minimale ondergrens zodat op het moment dat het weerstandsvermogen wordt aangesproken en de ratio onder de 1,0 komt, er ruimte is om een plan te maken hoe we het weerstandsvermogen weer aan te vullen.

Bijsturen op ratio weerstandsvermogen
We vinden het van belang om tijdig bij te sturen om te voorkomen dat het weerstandsvermogen onder onze norm komt of dreigt te komen. Als de ratio onder de 0,8 komt worden bij het volgende integrale afwegingsmoment van de ontwikkelingen/kaderbrief, programmabegroting of de jaarstukken afspraken gemaakt hoe bij te sturen om de ratio weer op het gewenste niveau te krijgen. Hierbij wordt het volgende afgesproken:

- positieve jaarrekeningresultaten prioritair bestemmen voor versterking van het weerstandsvermogen;
- het instellen van een spaarprogramma door toevoegingen te doen aan de beschikbare weerstandscapaciteit;
- bij beleid of besluiten met hoge risico's het risicoprofiel te verlagen voor zover mogelijk door het plan bij te stellen of de uitvoering uit te stellen.

10. Bijlagen

Bijlage 1. Termen en definities

Risicomanagement begint bij het spreken van dezelfde taal. Een juiste inschatting van een risico en haar effecten is alleen mogelijk wanneer we dezelfde definities hanteren. De belangrijkste definities worden hieronder beschreven.

Risico
Een risico is een onzekere en ongewenste gebeurtenis, waardoor het behalen van doelstellingen in gevaar komt. De doelstellingen kunnen onze strategische organisatie doelstellingen zijn maar ook kunnen ook operationele teamdoelstellingen zijn. Als er zekerheid is over het optreden van een gebeurtenis, dan is er géén sprake meer van een risico. Als de onzekere gebeurtenis geen gevolgen heeft voor het realiseren van doelstellingen, dan is er ook geen sprake van een risico. Binnen de definitie die in deze nota gehanteerd wordt gaan we uit van risico`s waarbij er een negatief effect is op een doelstelling. Een positief effect op de doelstelling is een kans, maar kan op dezelfde manier behandeld worden als een risico.

Risicomanagement
Risicomanagement is een set aan gecoördineerde activiteiten om onze organisatie te sturen en te beheersen met betrekking tot risico's. Dit zodanig dat er meer zekerheid bestaat dat doelen worden gerealiseerd. Met andere woorden, risicomanagement is het managen van onze doelen.

Risicomanagementproces
Dit is een continue en systematisch proces waarbij in een organisatie risico's worden geïdentificeerd, geanalyseerd en geëvalueerd om ze beheersbaar te maken.

Weerstandscapaciteit
Weerstandscapaciteit bestaat uit middelen en mogelijkheden die SamenTwente heeft om onverwachte, niet-begrote kosten of tegenvallende inkomsten (door bijvoorbeeld optreden van een risico) te kunnen dekken. Hierbij wordt onderscheid gemaakt tussen benodigde (geïnventariseerde risico's) en beschikbare weerstandscapaciteit (middelen en mogelijkheden). Daarnaast wordt er ook onderscheid gemaakt tussen incidentele en structurele weerstandscapaciteit. Onder incidentele weerstandscapaciteit wordt verstaan de capaciteit die SamenTwente heeft om eenmalige tegenvallers op te vangen. Onder structurele weerstandscapaciteit worden de middelen verstaan die permanent inzetbaar zijn om tegenvallers op te vangen.

Weerstandsvermogen
Weerstandsvermogen is de ratio van de beschikbare weerstandscapaciteit en de geïnventariseerde risico's. Dit ratio geeft aan in hoeverre SamenTwente in staat is om niet begrote tegenvallers op te vangen zonder dat onze taakuitvoering in gevaar komt. Het weerstandsvermogen is eigenlijk een indicator van robuustheid van onze begroting.

Bijlage 2. Categorieën en soorten risico's

De meest voorkomende en herkenbare risico`s zijn de financiële risico`s. Daarnaast zijn er ook andere categorieën van risico`s te onderscheiden. In deze nota wordt met risico`s alle categorieën bedoeld, tenzij er expliciet wordt gesproken over financiële risico`s. Te onderscheiden categorieën risico`s:

Risico	Omschrijving
1. Politiek/bestuurlijk/imago	Dit soort risico's houden verband met beleid en besluitvorming met onevenredige overheidsinterventies in reactie op een gebeurtenis of ontwikkeling waarbij de verantwoordelijkheid voor risicobeheersing min of meer vanzelfsprekend wordt opgevat als taak van onze organisatie.
2. Financieel	Financiële risico's hebben te maken met tegenvallers in geldstromen (meer lasten en/minder of baten) zoals rijksuitkeringen, aanbestedingen, leningen en garanties, verstrekken en aantrekken van subsidies
3. Juridisch/wettelijk	Juridische risico's doen zich voor als er sprake is van: het niet voldoen aan wet- en regelgeving waaronder strijd met de algemene beginselen van behoorlijk bestuur en inbreuken op grondrechten; het niet voldoen aan contractuele verplichtingen; juridische gebondenheid zonder dat daar een besluit aan ten grondslag ligt
4. Fraude en integriteit	Risico's samenhangend met bedoeld en onbedoeld niet-integer handelen door bestuurders, ambtenaren of externe partners.
5. Organisatorisch	Een organisatorisch risico houdt verband met de manier waarop de organisatie is ingericht en haar werkzaamheden uitvoert. Dit betreft dan de samenwerking, processen, procedures en systemen die tekort schieten voor de (bijzondere) omstandigheden op enig moment of het ontbreken daarvan.
6. Informatie	Risico's die betrekking hebben op de duurzame toegankelijkheid van informatie (informatiebeheer); betrekking hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie (informatiebeveiliging); verband houden met de verwerking van persoonsgegevens (privacy).
7. Maatschappelijk	Maatschappelijke risico's voor SamenTwente houden verband met zowel ontwikkelingen in de samenleving waarop wij in de uitvoering moeten reageren op een manier waarop we nog niet (voldoende) zijn voorbereid en/of toegerust, als risico's die ontstaan door eigen beleidskeuzes gericht op een maatschappelijk doel.

Naast de verschillende risico categorieën zijn risico`s ook in te delen in drie soorten: Te voorkomen/operationele risico`s, strategische risico`s en externe risico`s

Omschrijving	Operationele risico's	Strategische risico's	Externe risico's
Voorbeelden	Fouten in (geautomatiseerde) processen, ongeautoriseerde toegang tot systemen, onrechtmatig handelen	Nieuwe activiteiten, samenwerkingen, subsidies,(des) investeringen, afweging kansen en bedreigingen	Pandemie en/of epidemie, wet- en regelgeving, economische en demografische ontwikkelingen
Kenmerken	Dit zijn risico's die betrekken hebben op de interne processen, vaak betrekking op gedrag en zijn sterk te beïnvloeden met maatregelen.	Dit zijn risico's die afhankelijk zijn van de gestelde doelen in de programmabegroting en bij (grote) projecten. Deze zijn goed te inventariseren en er kan een afweging plaatsvinden tussen acceptatie of beheersing van risico's.	Dit zijn risico's die worden gekenmerkt doordat de oorzaak van het risico zich buiten ons invloedsfeer ligt.
Beheersing	Deze risico's moeten proactief gemanaged worden door (het regelmatig) checken van processen via interne controles en regels rondom gedrag en besluitvorming.	Bij deze risico's dient de kans van optreden dan wel de mogelijke impact te worden verkleind. Bij deze risico's dient een terugkerende dialoog te worden georganiseerd over de risicobereidheid en de gewenste maatregelen.	Vertaalslag maken naar concrete gevolgen voor de organisatie. Flexibiliteit van de organisatie. Scenario analyses en voldoende weerbaarheid organiseren.

Bijlage 3. Toelichting NEN-ISO 31000 principes

De NEN-ISO 31000 is een vrij toe te passen richtlijn en kan door de organisatie zelf op maat worden gemaakt. De NEN-ISO 31000 bestaat uit drie hoofdonderdelen; principes, raamwerk en het risicoproces. Deze bijlage geeft aanvullende informatie over de principes.

Principes NEN-ISO 31000

De principes zoals geïllustreerd in figuur geven richtlijnen van doelmatig en doeltreffend risicomanagement. Hieronder lichten we voor onze organisatie de belangrijkste principes toe en geven we ook aan hoe we deze in de praktijk toepassen.

Het doel van risicomanagement is het creëren en beschermen van waarde. Met andere woorden, goed risicomanagement verbetert de prestaties en ondersteunt het bereiken van doelstellingen.

a. Geïntegreerd: Integraal risicomanagement

Risicomanagement is pas waarde toevoegend als er sprake is van integraal risicomanagement. Hieronder verstaan we het breed invullen van risicomanagement. Dit betekent dat we bij risicomanagement niet alleen de wettelijke kaders volgen maar juist ook risicobewustzijn stimuleren. Risicomanagement is geen afzonderlijke activiteit maar maakt integraal onderdeel van alle processen (inclusief informatiebeveiliging en privacy). Dit houdt in dat we op alle niveaus risico's (alle processen) identificeren. Managers zijn verantwoordelijk voor risicomanagement in hun werkveld. Tegelijkertijd realiseren we ons ook dat bewust omgaan met risico's een onderdeel is van ieders werk. We richten ons bij integraal risicomanagement zoals toegelicht in onze ambitie op risicomanagement zowel op strategische risico's als operationele risico's. Hierbij lig de focus niet alleen op risico's met financiële impact maar ook op risico's **zonder** een direct financiële impact. Bijvoorbeeld imago-, fraude-, juridische- en bestuurlijke risico's. Om met deze brede bril naar risico's te kunnen kijken, zorgen we ervoor dat risico's identificeren een proces is waarbij meerdere disciplines bij betrokken zijn.

b. Gestructureerd

Een gestructureerde benadering van risicomanagement draagt bij aan consistente en vergelijkbare resultaten. Werken op basis van één risicomanagementkader (raamwerk) binnen de gehele organisatie draagt bij aan een gestructureerde aanpak. Onze aanpak is cyclisch en sluit aan op de bestaande processen. Hierbij wordt het ontstaan van aparte werkwijzen en eilandjes op het gebied van risicomanagement zoveel als mogelijk tegengegaan.

c. Dynamisch

SamenTwente is verantwoordelijk voor een breed scala aan maatschappelijke taken. De maatschappij is continue in beweging en dit heeft ook impact op wat er van onze organisatie verwacht wordt. Zowel de interne als de externe context van onze organisatie is dynamisch waardoor risico's kunnen ontstaan, veranderen maar ook kunnen verdwijnen. Ons risicomanagement anticipeert hierop, detecteert dit en reageert hier op een tijdige en passende wijze op. Risico's komen voor in al onze doelstellingen, denk aan onze inhoudelijke doelstellingen vanuit GGD Twente, Veilig Thuis Twente en OZJT. Maar ook aan doelstellingen uit onze projecten en de bedrijfsvoering. Deze doelstellingen veranderen periodiek. We houden ons risicomanagement dynamisch door een koppeling te leggen tussen doelen en risico's. Daarnaast is het eenmalig inventariseren en analyseren van risico's

onvoldoende. Het is een continue proces van identificeren, analyseren en evalueren. Bij wijzigingen in bijvoorbeeld de externe omgeving, als nieuwe wetgeving, is het noodzakelijk weer te kijken naar de risico`s en bijhorende maatregelen. Alleen dan is sprake van risicomanagement.

d. Menselijke en culturele factoren

Goed risicomanagement kan pas plaatsvinden als er aandacht is voor menselijk gedrag en cultuur. Deze elementen hebben namelijk invloed op alle aspecten van risicomanagement en op elk niveau. We zorgen ervoor dat bij onze organisatie op alle ambtelijke en bestuurlijke niveaus bereidheid en ruimte is om open over risico's (en fouten) te praten. We spreken elkaar aan als dat niet zo is. Risico's nemen is onvermijdelijk maar erover communiceren ook. Een goede dialoog, het gesprek, over risico`s en kansen zien wij als een belangrijke voorwaarde voor doeltreffend risicomanagement waarbij het spreken van dezelfde taal (definities) van belang is.

e. Continue verbetering

Eén van onze leidende principes is het zijn van een lerende organisatie. Dit betekent dat we ons risicomanagement continue verbeteren door leren en ervaring. Wie niet reflecteert op successen en fouten, stopt met leren. Door het gesprek over risico`s en kansen zien we ook eerder potentiële verbeterpunten wat bijdraagt aan het zijn van een lerende organisatie

Informatienota AB

Voorstel van het dagelijks bestuur
15 november 2024

Openbaar	Registratienummer	Datum
Openbaar	2024-000021	11 december 2024

Agendapunt	Onderdeel SamenTwente
C1	Bedrijfsvoering

Onderwerp
Beleidsstukken informatiemanagement, -beveiliging en privacy

Kennis te nemen van

1. Het Informatiebeleidsplan 2025-2028.
2. Het Informatiebeveiligingsbeleid 2025-2028.
3. Het privacy beleid 2025-2028.

Inleiding

SamenTwente is verantwoordelijk voor zeer privacygevoelige informatie. Gegevens van (kwetsbare) Twentse inwoners gaan door onze systemen en processen. Deze gegevens moeten veilig zijn en blijven. In uw vergadering van 16 oktober 2024 is onze I-visie 2024-2028 vastgesteld. Deze I-visie vloeit voort uit het ambitiedocument voor versterking informatiemanagement, -beveiliging en privacy en de per 2025 structureel toegekende begrotingsuitbreiding van € 1,23 miljoen. Door de begrotingsuitbreiding zijn we in staat om de basis meer op orde te brengen door te voldoen aan wet- en regelgeving, kwetsbaarheid te verminderen en sneller te anticiperen op nieuwe ontwikkelingen. Om aan onze ambities uitvoering te geven, hebben we ons (uitvoerings)beleid voor informatiemanagement, -beveiliging en privacy opgesteld. Deze beleidsstukken zijn door ons dagelijks bestuur op 15 november jl. vastgesteld.

Kernboodschap

1.1 Het is belangrijk om onze informatievoorziening op orde te brengen en te houden
Dit is van cruciaal belang want de informatiebehoefte van inwoners, cliënten, ketenpartners en medewerkers verandert continu. Maatschappelijke, technologische, wettelijke en organisatorische ontwikkelingen volgen elkaar in rap tempo op en worden steeds complexer. We willen op deze ontwikkelingen grip krijgen en hierop anticiperen door de komende jaren op drie ontwikkelsporen in te zetten. We willen inzetten op een stevige basis, we willen een digitale en wendbare organisatie zijn en we willen informatie gestuurd werken.

2.1 Informatiebeveiligingsbeleid vormt de basis voor een veilige informatievoorziening
SamenTwente ondersteunt en versterkt de inzet en activiteiten van gemeenten en samenwerkingspartners om inwoners van Twente gezond, veilig en vitaal te houden. Hierbij werken we dagelijks met kritische, vertrouwelijke en persoons-gerelateerde informatie. Informatieveiligheid is daarom van het grootste belang voor de organisatie. In ons informatieveiligheidsbeleid hebben we doelstellingen opgenomen, geven we inzicht in reikwijdte en inzicht in onder meer verantwoordelijkheden met betrekking tot informatiebeveiliging.

3.1 Het privacy beleid geeft inzicht in uitgangspunten hoe we privacygevoelige informatie verwerken en beschermen
SamenTwente werkt met veel privacygevoelige informatie. Denk hierbij aan gevoelige informatie bij Veilig Thuis Twente, bij de forensische dienstverlening en bij de JGZ. Het is belangrijk voor ons om deze informatie op de juiste wijze te verwerken en beschermen. Ook als we deze gegevens delen met ketenpartners of andere derden. We willen immers voorkomen dat deze gegevens in verkeerde handen terechtkomen, waardoor er misbruik van kan worden gemaakt. Met ons privacy beleid geven we inzicht in de beleidsuitgangspunten, geven we inzicht in wet- en regelgeving en hoe we omgaan met rollen en verantwoordelijkheden met betrekking tot privacy.

Communicatie
n.v.t.

Vervolg
- We geven via onze P&C cyclus periodiek inzicht in de uitvoering van de beleidsstukken.
- Het beleid zal ook vertaald worden in processen en procedures die in ons kwaliteitsmanagementsysteem worden uitgewerkt.

Bijlage(n)
1. Informatiebeleidsplan 2025-2028
2. Informatiebeveiligingsbeleid 2025-2028
3. Privacy beleid 2025-2028

Besproken

[tekst]

Enschede
11 december 2024

secretaris

drs. S. Dinsbach

voorzitter

drs. C.F.M. Bruggink

Samen Twente

Gezond, veilig vitaal

Informatiebeleidsplan 2025-2028

Managementsamenvatting

Waarom dit Informatiebeleidsplan?

- Het op orde brengen en houden van onze informatievoorziening is van strategisch belang. Want de informatiebehoefte van inwoners, cliënten, ketenpartners en medewerkers verandert continu. En maatschappelijke, technologische, wettelijke en organisatorische ontwikkelingen volgen elkaar in rap tempo op en worden steeds complexer.
- Deze ontwikkelingen hebben veel impact op de informatievoorziening van SamenTwente. Het leidt tot grote veranderingen voor onze organisatie. Dit vraagt ons om komende jaren extra stappen te zetten om de kansen van digitalisering beter te benutten en de risico's ervan zoveel mogelijk te beheersen.

Vastgestelde drie ontwikkelsporen voor de komende drie jaar:

- **Een stevige basis**: het opstellen en inrichten van Governance en Beleid, het werken binnen afgesproken kaders (Architectuur) en het harmoniseren van onze werkprocessen en applicaties.
- **Digitale en wendbare organisatie**: het ontwikkelen van een persoonlijke, toegankelijke dienstverlening, zaak- en procesgericht werken, integraal samenwerken en het ontwikkelen van de digitale vaardigheden van de medewerkers.
- **Informatiegestuurd werken**: informatiegestuurd werken is onderdeel van ons dagelijks werk. We werken aan groei in volwassenheid op gebied van informatiegestuurd werken.

Toekomstige vervolgactiviteiten:

- Structurele borging van het informatiebeleid binnen de organisatie na vaststelling van de koers en de ambitie. Dat doen we door te werken aan een organisatiebreed projectenportfolio. Dit stelt CMT en het bestuur in staat te sturen op de strategische koers, de prioritering van projecten en de bijbehorende capaciteit en middelen.
- Het opstellen van een projectenkalender waarin we één tot twee jaar vooruitkijken. Hierdoor sluiten we aan op de planning- & controlcyclus van SamenTwente.

Versiebeheer

Versie	Datum	Door	Omschrijving
0.1	04-10-2023	G. Roos	Concept informatiebeleid
0.2	08-11-2023	Olga Leever	Redactie tekstschrijver versie 1
0.3	15-11-2023	Olga Leever	Redactie tekstschrijver versie 2

Inhoudsopgave

1 Inleiding

De informatiebehoefte van inwoners, cliënten, ketenpartners en medewerkers verandert continu. Maatschappelijke, technologische, wettelijke en organisatorische ontwikkelingen volgen elkaar in rap tempo op. En de komende jaren neemt de snelheid en complexiteit van deze ontwikkelingen alleen maar verder toe. Deze ontwikkelingen hebben grote impact op de informatievoorziening van SamenTwente. Het op orde brengen en houden van onze informatievoorziening is van strategisch belang.

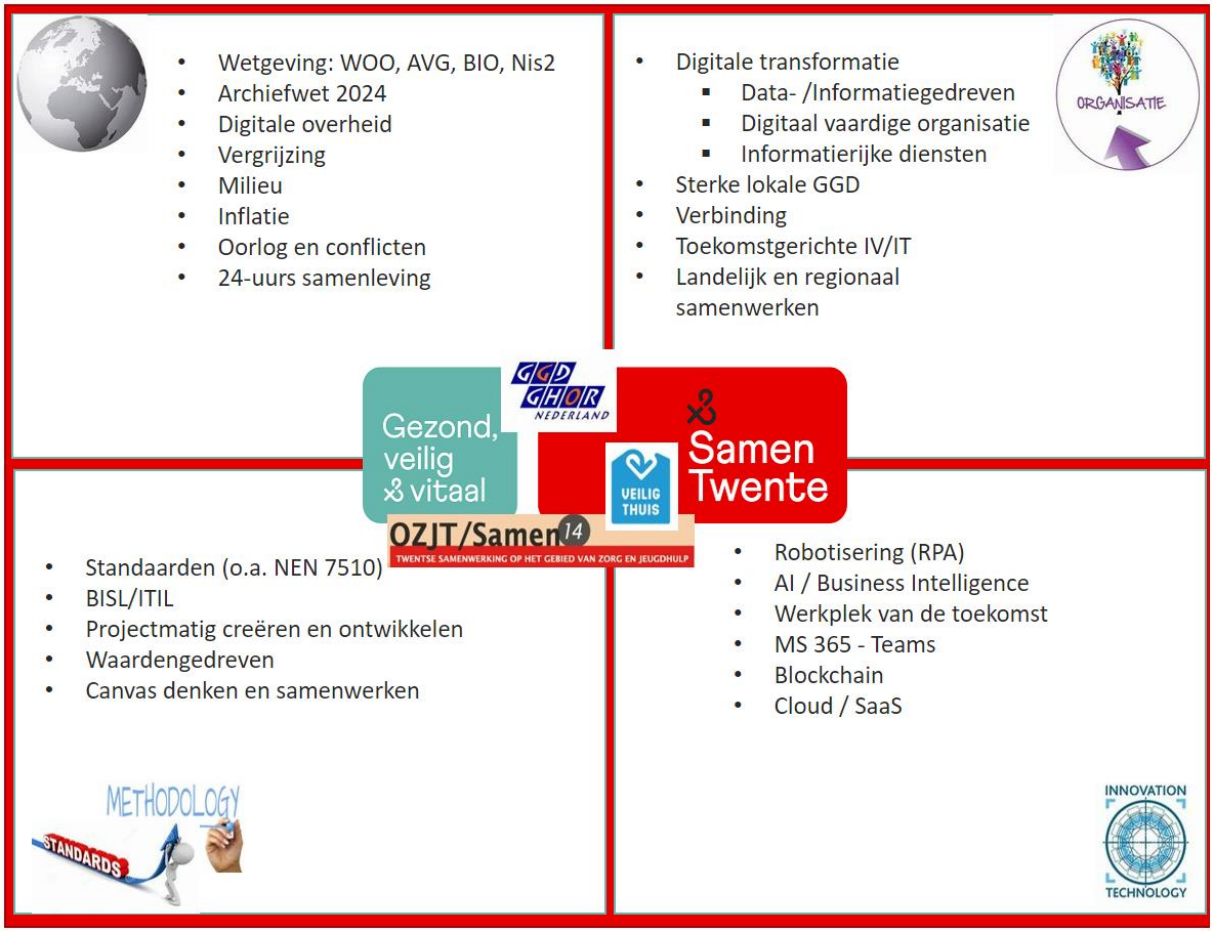
Vooruitblik 2024-2028
In dit informatiebeleid kijken we vooruit naar de periode 2024 – 2028. Wat zijn de nieuwe ontwikkelingen? En hoe geven we hier invulling aan? Je vindt ook de projecten voor de komende jaren in dit plan. We nemen ze op in het programma waar het CMT goedkeuring voor heeft gegeven.

Leeswijzer
In dit document vind je:

- de ambities en doelen van SamenTwente op strategisch niveau
- de belangrijkste ontwikkelingen op gebied van informatievoorziening
- de impact van deze ontwikkelingen op de organisatie
- de koers van SamenTwente hierin
- een advies over de benodigde kennis en kunde om deze opgave aan te gaan
- een projectenkalender, inclusief financiële vertaling (bijlage)

1.1 Relevante trends en ontwikkelingen

Wat zijn de ontwikkelingen in informatiebehoefte de komende jaren? En hoe zijn die ontwikkelingen van invloed op onze strategische koers? We zetten het in dit hoofdstuk voor je op een rij.



1.2 Externe ontwikkelingen

Cybercriminaliteit voorkomen

Ontwikkeling

Cybercriminaliteit komt ook bij ons voor. Zo heeft bij onze GGD begin 2021 datadiefstal plaatsgevonden. Daarbij zijn privégegevens van personen uit de systemen van de GGD gestolen en mogelijk verhandeld. Het ging om persoonsgegevens als de volledige naam, woonadres, geboortedatum, telefoonnummer en het burgerservicenummer (bsn). Criminelen misbruiken deze gegevens voor identiteitsfraude, phishing en oplichting. Zelfs de privégegevens van BN'ers, politici en beveiligde personen zijn in te zien en te misbruiken.

Actie voor ons

We willen voorkomen dat criminele organisaties of personen misbruik maken van vertrouwelijke (persoons)gegevens. Dit is mogelijk door het versterken van de informatiepositie, actualiseren, regionaal afstemmen en consequent uitvoeren van beleid.

Extra eisen aan organisaties door de Wet open overheid

Ontwikkeling

Op 1 mei 2022 is de nieuwe Wet open overheid (Woo) ingegaan. Doel is het overheidshandelen (nog) transparanter te maken. De Woo is de opvolger van de Wet openbaarheid van bestuur (Wob). Mensen kunnen verzoeken indienen om informatie openbaar te laten maken. Daarnaast bepaalt de Woo dat een aantal documenten vanuit onze organisatie proactief openbaar gemaakt moet worden. Daarbij gaat het bijvoorbeeld om documenten rond besluitvorming. 'De basis op orde' is een voorwaarde om aan deze actieve openbaarmakingsplicht te kunnen voldoen. Dit omvangrijke traject vindt stapsgewijs plaats de komende tien jaren.

Acties voor ons

- De Woo bepaalt, dat informatie 'duurzaam toegankelijk' moet zijn. Omdat het om digitale informatie gaat, stelt dit extra eisen aan het gecontroleerd opslaan en vernietigen van bestanden. Ook zijn er extra eisen voor metadateren: bestanden voorzien van kenmerken over context en inhoud.
- Zaken/processen moeten we classificeren naar hun belang (BIV: beschikbaarheid, integriteit, vertrouwelijkheid). Ook moeten we elk document labelen naar de mate van vertrouwelijkheid: intern/ extern vertrouwelijk, actief/passief openbaar, anonimiseren. En dus moeten we alle processen hierop aanpassen.
- Aan deze aanpassingen gaat een beleidswijziging vooraf, inclusief governance, plancyclus en risicomanagement.

Wijziging Archiefwet

Ontwikkeling

De overbrengingstermijn wijzigt van 20 jaar naar 10 jaar. Het doel van deze maatregel is, dat belangrijke (digitale) overheidsinformatie beter bewaard en vindbaar blijft - en daarmee bruikbaar voor huidige en toekomstige generaties. Digitalisering leidt namelijk ook bij de overheid tot een explosieve groei van informatie: van documenten en databestanden tot e-mails en websites. Bovendien raakt informatie verspreid over allerlei verschillende systemen die draaien op software die snel veroudert.

Actie voor ons

Informatie die we blijvend moeten bewaren, moeten we selecteren en overbrengen naar archiefdiensten: eDepots of archiefsystemen van gemeentes waar we op zouden kunnen aansluiten. Daar zorgen experts dat de digitale bestanden leesbaar blijven. Dat betekent dat we ons analoge en digitale archief versneld moeten overgedragen.

Blijvende aandacht voor de Algemene Verordening Gegevensbescherming

Ontwikkeling

Sinds 2018 geldt de AVG. Dit is de wettelijke basis voor de redenen waarom de overheid persoonsgegevens mag verwerken. Ook geeft de AVG burgers het recht om de overheid te vragen hun persoonsgegevens in te zien, te laten corrigeren of te verwijderen. Binnen onze organisatie is nog onvoldoende bewustwording hoe om te gaan met (bijzondere) persoonsgegevens. En dus vormt bij het implementeren van nieuwe wetten, applicaties en processen de AVG een dagelijkse uitdaging voor ons. Want om de wet goed te kunnen uitvoeren, is een gerichte informatiehuishouding nodig. Dat houdt in dat de basis op orde moet zijn, met borging hoe we informatie vastleggen. En waarbij de beveiliging

en privacy-onderwerpen goed zijn ingevoerd in de processen en applicaties. Bovendien ligt er met de introductie van de verantwoordingsplicht een stevige last op de schouders van publieke organisaties.

Acties voor ons

We hebben blijvend aandacht voor informatiebeveiliging en privacy door het uitvoeren van risico-inventarisaties (DPIA), een verwerkingsregister en andere maatregelen.

Baseline Informatiebeveiliging Overheid

SamenTwente moet voldoen aan wet- en regelgeving en normenkaders als de NEN7510, de BIO en NIS2. Aan de hand van risicoanalyses zal onderzocht moeten worden voor welke informatie en informatiesystemen een hoger beveiligingsniveau moet worden gehanteerd en welke aanvullende maatregelen hiervoor moeten worden getroffen. Het implementeren van de BIO/NEN7510/Nis2 is géén eenmalige actie, maar een continu proces.

1.3 Organisatorische ontwikkelingen

Van papierloos naar documentloos

Ontwikkeling

Processen zijn afgelopen jaren in rap tempo gedigitaliseerd. In deze processen worden nog steeds veel (digitale) documenten geproduceerd, bijvoorbeeld in Word en PDF. De volgende stap is dat documenten worden vervangen door sets aan data en metadata.

Acties voor ons

We moeten informatiesystemen anders inrichten. Hoe, dat staat beschreven in het adviesrapport Datamanagement. Ook vraagt deze ontwikkeling om nieuwe werkwijzen en uitgangspunten ten aanzien van (digitale) archivering.

Altijd en overal verbonden

Ontwikkeling

Medewerkers stellen steeds hogere eisen aan voorzieningen die het mogelijk maken om tijd- en plaats onafhankelijk te kunnen werken. De coronacrisis heeft de behoefte nog meer aangewakkerd en versnelling aangebracht.

Actie voor ons

De inzet van cloudapplicaties en Microsoft 365 als digitaal communicatiemiddel en samenwerkingstool zijn de nieuwe norm. Hier hebben we nog geen vastgesteld beleid voor.

Investeren in 21e-eeuwse vaardigheden

Ontwikkeling

Investeren in digitale vaardigheden is nodig om de voordelen van de technologieën te benutten en de risico's ervan te beperken, nu en in de toekomst. Deze vaardigheden worden ook wel 21e-eeuwse vaardigheden genoemd. Dit zijn generieke vaardigheden en de kennis, inzicht en houdingen die nodig zijn om te functioneren in en bij te dragen aan de huidige en toekomstige samenleving en organisatie.

Actie voor ons

Hoe we dit concreet invullen, lees je in hoofdstuk 3.2 'digitale en wendbare organisatie.'

Flexibel inspelen op behoeften

Ontwikkeling

De trends en ontwikkelingen gaan snel. Als organisatie is het belangrijk om in te spelen op de snel groeiende digitalisering.

Acties voor ons

Als dienstverlener voor GGD Twente, VTT en OZJT moeten wij voldoen als standaarden zoals NEN 7510. Dit is het certificaat dat je ontvangt als je een managementsysteem voor informatiebeveiliging hebt opgezet. Daarnaast moeten wij ons snel kunnen aanpassen aan de veranderende informatiebehoeften vanuit de inwoners, cliënten en wet- en regelgeving. En daarbij horen nieuwe werkvormen als integraal samenwerken en kortere cycli om (deel) producten op te leveren, oftewel Agile werken.

1.4 Technologische ontwikkelingen

SaaS-oplossingen

Ontwikkeling

Lange tijd hadden organisaties op de eigen locatie of eventueel in een samenwerkingsverband een serverpark in gebruik met daarop allerlei programma's. Deze tijd lijkt langzaam maar zeker voorbij. Steeds meer leveranciers ontwikkelen nieuwe software alleen nog maar voor de 'cloud'. Deze ontwikkeling heeft gevolgen voor de problemen en uitdagingen bij SamenTwente.

Acties voor ons

Als we kiezen voor een SaaS-oplossing, verzorgt de SaaS-leverancier het technisch beheer van de applicatie. Dit valt dan buiten de (directe) verantwoordelijkheid van SamenTwente. En dat vraagt om extra eisen aan de beveiliging van de gegevens, zoals bijvoorbeeld verwerkersovereenkomsten. De gegevens worden immers buitenshuis verwerkt. Een ander aandachtspunt is hoe gegevens vanuit een SaaS-oplossing beschikbaar zijn voor andere applicaties.

Robotisering en kunstmatige intelligentie (KI)

Ontwikkeling

Robotisering zorgt ervoor dat taken die nu nog als vanzelfsprekend worden uitgevoerd door mensen, op termijn vervangen worden door technologische processen. Door de robotisering veranderen of verdwijnen veel beroepen in de nabije toekomst. Daarnaast hebben we te maken met Kunstmatige intelligentie (KI): een verzamelnaam voor machines en systemen die menselijk denkvermogen nabootsen. Het legt verbanden en voert taken uit op basis van complexe algoritmes en wiskundige formules. Zo kan kunstmatige intelligentie handelingen vereenvoudigen of ze zelfs helemaal overnemen van de mens.

Actie voor ons

We zouden in de toekomt robotisering kunnen inzetten voor repeterende werkzaamheden. Maar dit is nu nog niet toepasbaar binnen onze organisatie.

Data en algoritmes

Ontwikkeling

Een grote hoeveelheid data is een belangrijke grondstof voor innovatie, en daarmee voor nieuwe economische en maatschappelijke kansen. Iedereen wil er dus zoveel mogelijk van hebben. Niet voor niets wordt gezegd 'data is het nieuwe goud'. De algoritmes zijn de 'mijnwerkers'. De informatie die uit de veelheid aan data kan worden gegenereerd zijn de diamanten.

Actie voor ons

Op dit moment is dit niet relevant voor ons, maar het is de moeite van een onderzoek waard in de toekomst.

2 Drie sporen: huidige en gewenste situatie

Nu we de relevante ontwikkelingen hebben besproken, gaan we in dit hoofdstuk in op de huidige en de gewenste situatie. Dat doen we aan de hand van drie ontwikkelsporen. Met deze sporen kijken we van buiten naar binnen: van de ontwikkelingen naar de informatiehuishouding van SamenTwente.

2.1 De drie sporen

Dit zijn de drie ontwikkelsporen:

Per spoor hebben we de huidige en gewenste situatie (ambitie) vastgesteld. Dit geven we weer aan de hand van een vijfpuntsschaal. Deze schaal laat zien hoe ver de organisatie op dit gebied ontwikkeld is: hoe volwassen zijn we? En hoe staat het met de informatiehuishouding van SamenTwente? Bij ieder spoor geven we aan waar we staan en waar we naar toe willen. Vervolgens geven we een toelichting op het spoor en op de benodigde acties om het verschil tussen de huidige en gewenste situatie te overbruggen. We maken een onderscheid in de volgende classificering (mate van volwassenheid):

Ad-hoc	●○○○○	*Reactief, rollen en verantwoordelijkheden niet benoemd. Grote afhankelijkheid van enkele medewerker(s).*
In control	●●○○○	*Er is overzicht, sturing op beheersbaarheid. Rollen en verantwoordelijkheden zijn benoemd. Streven naar voldoen aan verplichtingen.*
Optimaliseren	●●●○○	*Procesverbetering als drive (lean efficiency). Er wordt aantoonbaar aan verplichtingen voldaan.*
Professionaliseren	●●●●○	*Continu verbeteren met de organisatie doelstellingen als leidraad. Processen zijn beschreven.*
Adaptief, optimaal	●●●●●	*Maximaal wendbaar. Maatschappelijke verandering en technologische ontwikkelingen als continuïteit. Toekomstgericht, proactief.*

2.2 Een stevige basis

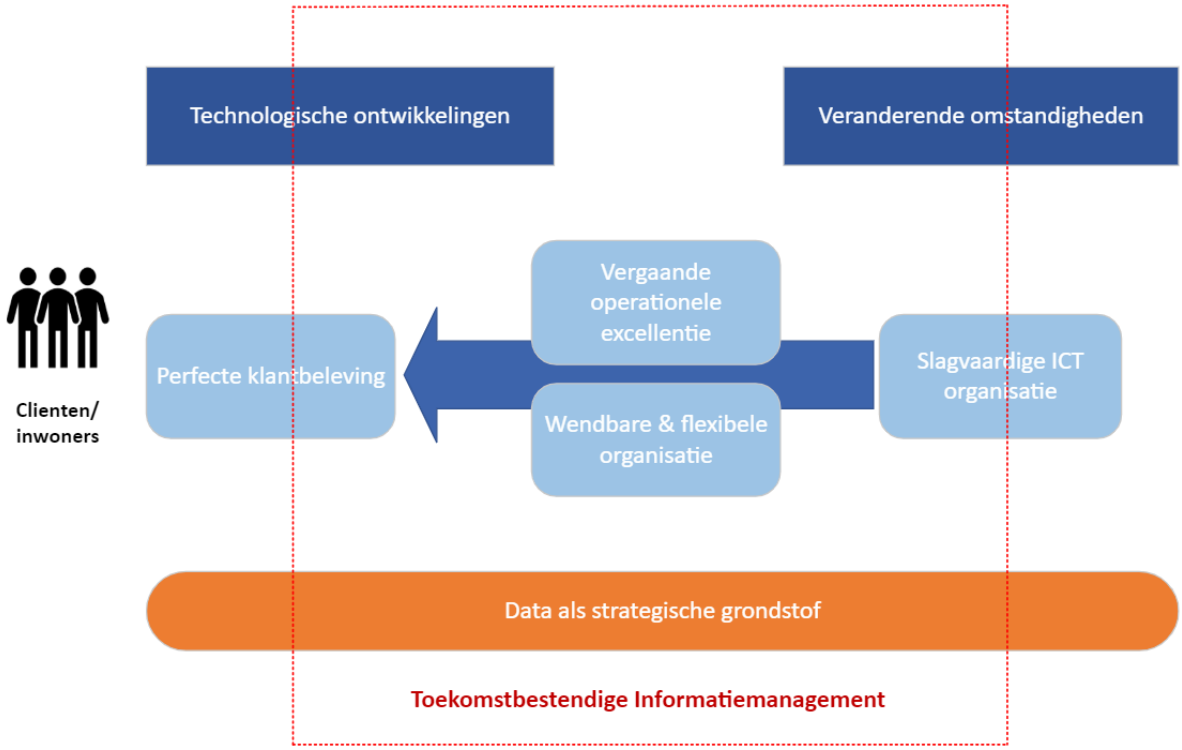
Het opstellen van een Informatiebeleidsplan biedt kansen om processen opnieuw vorm te geven, te standaardiseren en het eigenaarschap goed te beleggen. Dit heeft een bijkomend positief effect: het applicatielandschap wordt onder de loep genomen en kan opnieuw kan worden vormgegeven, gericht op toekomstbestendig gebruik van wet- en regelgeving.

Uitgangspunten

- Naleving van wet- en regelgeving
- Weerbaarheid en continuïteitsbeheer
- Continu de juiste prioriteit en balans zoeken
- Integrale managementverantwoordelijkheid is de basis

We creëren een stevige basis door:

1. Governance-, Risico- en Compliancebeleid op te stellen
2. Harmoniseren van werkprocessen en applicaties
3. Werken onder architectuur



Governance, Risico en Compliance

Huidige volwassenheid ●○○○○
Gewenst, ambitie ●●●○○

Wat is de huidige situatie?
Technologische ontwikkelingen volgen elkaar in snel tempo op en er komen nieuwe wetten en regels aan. Ook werken we steeds meer samen met onze ketenpartners. En dat vraagt veel van onze informatievoorziening. Dit biedt kansen, maar brengt ook (nieuwe) risico's met zich mee. Als we kijken naar de huidige situatie van onze informatievoorziening binnen SamenTwente, dan constateren wij:

- Organisatie- en functionele silo's
- Gebrek aan overzicht
- Informatie versnipperd door de hele organisatie
- Fragmentatie
- Onnodige complexiteit
- Onvoldoende integriteit
- Cultuur

Wat willen we bereiken?
We willen **een geïntegreerde Governance, Risk and Compliance (GRC)-aanpak implementeren** die ons helpt om onzekerheid aan te pakken, integer te handelen en doelstellingen op betrouwbare wijze te bereiken met behulp van een risicobewuste cultuur. Dit is noodzakelijk gezien het belang van een goede informatievoorziening en de strategische rol van IM&T daarin

GRC is een overkoepelende term die verwijst naar de manier waarop wij onze bedrijfsvoering kunnen inrichten om te voldoen aan wet- en regelgeving, risico's te beheersen en onze doelen te bereiken. Een GRC-oplossing kan ons helpen bij het voldoen aan een hele set van normen en wetgeving rondom informatiebeveiliging, veiligheid, kwaliteit enzovoort. Deze oplossing biedt ondersteuning bij het voldoen aan allerlei normen en wetten, maar ook bij de financiële verantwoording die wij moeten doen.

Wat gaan we daarvoor doen?
- Een Governance Board inrichten binnen SamenTwente voor toetsing en naleving van onze principes, richtlijnen en uitgangspunten op het gebied van de informatievoorziening.
- Duidelijke afspraken maken over de levenscyclus van informatie en documenten.
- Duidelijke ontwerpprincipes opstellen: classificatie, labels, metadata enzovoort.
- Samen met Architectuurprojecten toetsen op vastgestelde kaders, uitgangspunten en richtlijnen.
- Een Change Advisory Board (CAB) oprichten om wijzigingsverzoeken te kunnen beoordelen op impact en kosten- batenanalyse, voordat deze in de systemen worden doorgevoerd.

Harmoniseren van werkprocessen en applicaties
Huidige volwassenheid ●○○○○
Gewenst, ambitie ●●●○○

Wat is de huidige situatie?
Binnen SamenTwente speelt de vraag hoe wij onze informatie toegankelijk kunnen maken. Door de groei van de hoeveelheid informatie binnen de organisatie wordt het steeds moeilijker om hier grip op te krijgen. Vragen die we op dit moment moeilijk kunnen beantwoorden, zijn:
- Hoe zorg ik dat informatie (snel) vindbaar, actueel, relevant, toegankelijk en bruikbaar is?
- Hoe koppel ik informatie uit verschillende bronnen aan elkaar?
- Hoe zorg ik dat de juiste informatie voor de juiste mensen op het juiste moment beschikbaar en toegankelijk is?
- Hoe kan informatie mijn organisatie efficiënter, servicegerichter, wendbaarder en innovatiever maken?

Dit heeft zijn weerslag op de inrichting van ons huidige informatielandschap: processen, informatiestromen, applicaties en infrastructuur. Het is van belang de samenhang tussen deze vier invalshoeken in kaart te brengen, zodat we inzichtelijk krijgen hoe wij onze werkprocessen en de ondersteunende applicaties kunnen harmoniseren.

Wat willen we bereiken?
Informatiemanagement is het beheren en managen van informatie die ondersteuning biedt bij het behalen van onze strategische doelstellingen. In dit proces wordt de informatiebehoefte die vanuit de primaire processen en de IT ontstaan, beantwoord met de informatievoorziening. De informatievoorziening is een verzameling van activiteiten die SamenTwente als geheel ondersteunt vanuit verschillende niveaus:

- Strategisch: informatiestrategie en planning
- Tactisch: businessproces, informatielandschap
- Operationeel: produceren van informatie

Binnen SamenTwente zijn primaire en ondersteunende processen ingericht, die elk hun eigen informatiebehoefte hebben. Vanuit die processen en organisatie ontstaat een informatiebehoefte waaraan voldaan moet worden. Onze processen moeten ervoor zorgen dat het gebruik, onderhoud en beheer volgens afspraak en verwachtingen wordt uitgevoerd. Ook moet dit goed worden begeleid. Dat betekent dat we kritisch moeten kijken naar onze huidige processen: waar zijn optimalisatieslagen mogelijk? Ditzelfde geldt voor onze applicaties.

Wat gaan we ervoor doen?
- Onze processen en het informatielandschap (applicaties en infrastructuur) brengen we in kaart en verbeteren de kwaliteit van onze data zodat ze geschikt zijn voor hergebruik. Zo brengen we onze informatie op orde.
- Benoemen van proceseigenaren en daarbij procesmanagement inrichten.
- Investeren in een centraal platform, waarbij architectuur, processen en normeringen aan elkaar gekoppeld worden. Zo maken we inzichtelijk hoe de relaties en afhankelijkheden liggen. Bij een aanpassing of wijziging wordt direct inzichtelijk wat de gevolgen zijn voor het proces en de informatiestromen.
- Zorgen dat informatie vindbaar en beschikbaar is voor iedereen die over die informatie mag beschikken.

2.3 Werken onder architectuur

Huidige volwassenheid ●○○○○
Gewenst, ambitie ●●●○○

Wat is de huidige situatie?
Veranderingen in ons informatielandschap vinden niet altijd plaats in samenhang. Hierdoor kunnen we onze strategie en doelen niet altijd zo goed mogelijk realiseren.

Wat willen we bereiken?
We stellen een toetsingskader op die als meetlat wordt gebruikt voor toekomstige keuzes. Dit noemen we ‘werken onder architectuur’. Bij deze manier van werken zijn besturing, organisatie, processen en ondersteuning in samenhang ingericht.

Deze vier invalshoeken vormen de pijlers voor het werken onder architectuur. Architectuur gaat niet alleen over beheersen, maar vooral ook over versnellen van ontwikkeling door hergebruik, heldere kaders, afbakenen etc. Architectuur helpt ook bij het omgaan met onzekerheden en het realiseren van oplossingen die aanpasbaar en wendbaar zijn. Wij gaan projecten binnen deze afgesproken kaders uitvoeren, waarbij we ook rekening houden met informatiebeveiliging en privacy. Zo borgen en bewaken we dat veranderingen in ons informatielandschap in samenhang plaatsvinden, waardoor we onze strategie en doelen maximaal realiseren.

Onze uitgangpunten bij werken onder architectuur

Wij hanteren een aantal principes als leidraad. Deze principes geven kaders bij alle veranderingen in onze omgeving.

- **Stabiliteit en continuïteit van onze dienstverlening voorop**
  Een stabiel, betrouwbaar en toekomstbestendig IT-landschap is een belangrijke voorwaarde voor de uitvoering van onze maatschappelijke taak en het bieden van de juiste dienstverlening.
- **ICT-omgeving tijdig en geleidelijk vernieuwen**
  Dit principe ondersteunt de ambitie om meer proactief dan reactief te vernieuwen en dit op een beheersbare manier te doen. Het brengt het portfolio in balans en geeft focus op de langere termijn.
- **ICT-innovatie is primair gericht op het realiseren van onze opdracht en bedrijfsdoelstellingen**
  Ons doel om cliënt en medewerker voorop te stellen rechtvaardigt functionele innovatie. Het doel van de innovaties moet altijd het bedrijfsbelang dienen, de vorm is kleinschalige beproeving.
- **We kiezen voor security & privacy by design/default**
  Bij het ontwerpen en inrichten van processen en systemen passen we informatiebeveiliging en privacy-borging toe.
- **Continue verbetering van processen**
  Elke dag beter presteren: daar streven we naar. Beter presteren vergroot onze verandercapaciteit, verlaagt kosten, realiseert sneller baten, verhoogt tevredenheid bij cliënten en medewerkers en helpt onze opdracht en bedrijfsdoelstellingen te realiseren.
- **De business is leidend bij onze eigen IM&T onder functionele sturing van Bedrijfsvoering**
  De business is leidend bij het informatievoortbrengingsproces, maar wel onder functionele sturing en centrale kaderstelling van Bedrijfsvoering. De wijze waarop de IM & T-organisatie is ingericht, ondersteunt en stimuleert de samenwerking om de gemeenschappelijke doelstelling te realiseren, waarbij de cliënt altijd centraal staat.
- **We gaan uit van vakmanschap van medewerkers. Daarbij past vertrouwen en mandaat**
  Vertrouwen in vakmanschap is een belangrijk principe. Binnen IM&T werken we met professionals die in hun werkzaamheden vertrouwen en mandaat krijgen. De organisatie stelt zo de medewerker centraal.
- **We bouwen aan een wendbaar en beheersbaar informatielandschap**
  Wij werken onder architectuur aan vereenvoudiging en wendbaarheid van het informatielandschap om sneller te kunnen reageren op veranderingen. Met gestandaardiseerde, ontkoppelde en vervangbare bouwblokken creëren we een wendbaar en beheersbaar landschap, zowel in infrastructuur als applicaties.
- **We realiseren ICT met bewezen technologieën**
  Bewezen technologieën zorgen voor lagere risico's en betere voorspelbaarheid. Binnen ons technologiebeleid toetsen we in het architectuurproces. Hiertoe rekenen wij overigens ook technologieën op basis van overheids-, open en marktstandaarden.
- **Hergebruik gaat boven standaardoplossingen. Standaardoplossingen gaan boven maatwerk**
  Bij het (her)invullen van functionele wensen is dit de prioritering bij het maken van een keuze:
    1. hergebruik

2. standaardoplossing
3. maatwerk.

Onder hergebruik verstaan we herhaalde inzet van middelen en functionaliteiten uit de organisatie verstaan, maar ook die van keten- en landelijke bouwstenen.

- **Gegevens leggen we eenduidig en eenmalig vast voor meervoudig gebruik**
  We passen kaders en architectuur voor datamanagement toe bij het ontwerpen en inrichten van de informatiehuishouding, waaronder taken, verantwoordelijkheden en bevoegdheden, dataprocessen en systemen. Dit wil zeggen datamanagement 'by design/default'.

Wat gaan we ervoor doen?

- De Nederlandse Overheid Referentie Architectuur (NORA) gebruiken we als referentie-architectuur. Daarnaast kiezen we voor vastgestelde standaarden van het Forum Standaardisatie en VNG.
- Onze processen en informatie brengen we op orde. En we verbeteren de kwaliteit van onze gegevens, zodat ze geschikt zijn voor hergebruik.
- We werken langs verschillende sporen aan een hogere volwassenheid. Daarbij zijn onze visie en ambities onze leidraad.
- We ontwikkelen een gezamenlijk projectenportfolio. We beginnen met projecten met een IM&T-component. Hiermee krijgen we grip op de prioritering en uitvoering van de verschillende projecten binnen onze organisatie.
- We passen portfoliomanagement toe. De ambitie is groot om diverse projecten op te pakken en te implementeren. Dat vraagt een totale veranderopgave, die veel van onze organisatie vraagt. Er zitten grenzen aan ons realisatievermogen. Niet alles kan tegelijkertijd: we moeten keuzes maken. En bij het maken van die keuzes geeft het informatiebeleidsplan de meerjarige richting op hoofdlijnen. Daarbij blijft het belangrijkste doel: zorgen voor continuïteit en stabiliteit.
- We maken periodiek afgewogen keuzes: met welke projecten gaan we van start? Daarbij houden we rekening met prioriteit en realiseerbaarheid op basis van beschikbare middelen en de schaarse resources. Het is namelijk belangrijk om te bedenken dat we de komende tijd maar zeer beperkte ruimte hebben om (nieuwe) initiatieven te starten. Dat komt onder andere door een aantal grote doorlopende projecten en de continue externe vraag naar veranderde en nieuwe wet- en regelgeving.
- De grote veranderopgave is alleen mogelijk als we zorgen voor meer capaciteit. Hiervoor versterken we ons capaciteitsmanagement, zodat we nog eerder inzicht hebben in de vraag. De betrokken bedrijfsonderdelen stellen hiertoe strategische personeelsplannen op, waarbij de veranderagenda, het beschikbare budget en de benodigde expertises in verandercapaciteit leidend zijn. Belangrijk is dat dit tijdig gebeurt: werving en inwerken kosten tijd en vragen een investering. Ook vraagt het om meebewegen van de dienstverlening vanuit leveranciers om de gewenste snelheid in verandertrajecten te bewerkstelligen.

2.4 Digitale & wendbare organisatie

Huidige volwassenheid ●●○○○
Gewenst, ambitie ●●●●○

Uitgangspunten

- Onze dienstverlening is digitaal waar het kan, persoonlijk waar het moet
- Afgestemd op de behoefte van de medewerker en de cliënt
- SamenTwente is er voor iedereen
- Dienstverlening is van iedereen
- We sluiten aan bij landelijke ontwikkelingen

- Onze cliënten hebben regie op hun eigen gegevens
- We vragen niet meer gegevens uit dan nodig
- We werken zaak- en procesgericht
- We werken integraal samen

Wat is de huidige situatie?

Op dit moment wordt informatievoorziening verantwoord beheerd met beperkte capaciteit en middelen. Het noodzakelijke wordt gedaan, maar anticiperen is moeilijk. Voor veel projecten zijn we als organisatie afhankelijk van één of enkele personen met de benodigde expertise. Er zijn veel 'eenpitters' binnen onze organisatie. Er is maar een select aantal medewerkers met de benodigde kennis die voor de meeste projecten gevraagd worden En dat maakt ons, en dus ook team IM & T, kwetsbaar. Door een uiterste inspanning hebben we een basis gelegd. Maar deze is nog niet op orde, laat staan dat we kunnen spreken van een wendbare organisatie. Er is behoefte aan concrete plannen en een blik vooruit.

Wat willen we bereiken?

Professionalisering

De komende jaren werken we verder aan het professionaliseren van Informatiemanagement, IV & P en functioneel beheer. Een plan met daarin een cloudstrategie is nadrukkelijk gewenst. Focus ligt hierbij op efficiënter werken, digitaal samenwerken in de keten en stoppen met verouderde technieken en componenten.

Toegankelijkheid voor iedereen

Ieder mens heeft het recht om te leven als ieder ander en mee te doen in de maatschappij. Gebruikmaken van de mogelijkheden die het internet, mobiele devices en smartphones bieden, hoort daar natuurlijk bij. Juist daarom is het belangrijk dat digitale dienstverlening toegankelijk is voor iedereen.
Met het digitaliseren van de samenleving ontstaan nieuwe mogelijkheden om digitaal contact tussen SamenTwente en de inwoners te hebben. Denk hierbij aan chat, videobellen en sociale media. Hierbij is omnichannel dienstverlening de uitdaging: de verschillende kanalen met elkaar verbinden om een integraal klantbeeld te krijgen. Inwoners hebben daarbij recht op regie op eigen gegevens. Ook willen we voorkomen dat we meerdere keren vragen naar gegevens die al bij ons bekend zijn.

Heldere processen

Bij proces- en zaakgericht werken verdelen we onze gemeentelijke taken en zorgtaken onder in heldere processen. De komende tijd benutten we om onze processen helder te krijgen.
We maken hierbij gebruik van de gestelde kaders binnen Architectuur om onze processen te stroomlijnen met landelijke standaarden, zodat we meer wendbaar en flexibel worden. De enorme hoeveelheid diensten en producten en de complexiteit ervan maken het nodig om de werkzaamheden vooral te ordenen vanuit een klantperspectief. We werken steeds meer in ketens, waardoor het procesbesef in de organisatie moet gaan groeien. De medewerkers denken nu nog teveel in applicaties en systemen en niet in processen.
Uiteraard brengen we de processen niet alleen in beeld – we verbeteren ze ook. Zo maken we ze beter beheersbaar en aanpasbaar.

Ontwikkeling zaakgericht werken

We gaan verder met de ontwikkeling van het zaakgericht werken. Want de dienstverlening verloopt steeds meer digitaal. Collega's werken vaker 'op afstand'. En procesgericht werken wordt steeds belangrijker. Bij dit alles speelt zaakgericht werken een sleutelrol. Zaakgericht werken maakt onder meer dit mogelijk:

- inrichten van onze sturing
- geeft meer helderheid over proces en voortgang van onze dienstverlening
- sluit aan op landelijke ontwikkelingen (waaronder Woo) en voorzieningen
- op een goede wijze archiveren.

Hierbij kiezen we voor decentraal en specifiek. Dit betekent dat we het zaakgericht werken afstemmen op de ondersteuning die binnen het proces nodig is. Met een centrale en generieke ondersteuning waar dat nodig is.

Investeren in digitale vaardigheden

Dit vraagt ook wat van de digitale vaardigheden van de medewerkers. Beperkte digitale vaardigheden zorgen voor risico's op gebied van informatiebeveiliging en privacy. Kansen van digitalisering worden niet (voldoende) benut. Komende jaren investeren we daarom extra in de 21e-eeuwse vaardigheden van de organisatie. Het verhogen van digitale vaardigheden heeft ook een positief effect op efficiëntie en effectiviteit van de werkzaamheden en processen. We investeren al in de adoptie van Microsoft 365 en Teams ter bevordering van het digitaal en tijd- en
plaat onafhankelijk (samen)werken. Het is tevens van belang om samen met HR een programma te ontwikkelen om de vaardigheden blijvend te trainen, denk bijvoorbeeld aan een fysieke en/of elektronische leeromgeving voor medewerkers.

Wat gaan we ervoor doen?

- Doorlopend investeren in 21e-eeuwse vaardigheden van de collega's, in nauwe samenwerking met HR.
- Cloudtoepassingen als dit voor ons meerwaarde biedt.
- Digitaal en tijd- en plaats onafhankelijk samenwerken.
- De mogelijkheden van InProces als zaaksysteem onderzoeken.
- De kansen van landelijke ontwikkelingen (VNG, GGD GHOR) volgen en onderzoeken.
- Concrete (jaar)plannen maken en samenwerking en kennisdeling stimuleren.
- Onze processen en werkwijzen optimaliseren.

2.5 Informatiegestuurd werken

Huidige volwassenheid ●○○○○
Gewenst, ambitie ●●●○○

Uitgangspunten

- We zetten sturingsinformatie in om ons beleid, dienstverlening en bedrijfsvoering te verbeteren.
- We werken vanuit een centrale visie en aanpak.
- We nemen ruimte om kleinschalig te experimenteren, leren en stap voor stap te ontwikkelen.
- We werken continu aan het verbeteren van de kwaliteit van onze data.
- We houden oog voor vraagstukken op gebied van ethiek en privacy.

Wat is de huidige situatie?

De gegevens die wij produceren en verwerken bieden een schat aan informatie. De vraag is hoe we de juiste informatie uit deze data naar boven halen. En hoe we deze informatie vervolgens in kunnen zetten om ons beleid, onze dienstverlening en onze interne processen verder te verbeteren. Op dit moment experimenteren we gefragmenteerd met data en worden de eerste dashboards ontwikkeld. Met name in het sociaal domein worden al stappen gezet. Zoeken naar de juiste gegevens kost veel tijd. Data zit in verschillende systemen en sluit meestal niet goed aan. Het is nog vaak 'sturen in de mist'. Er

wordt op dit moment nog niet gewerkt vanuit een centrale aanpak of visie. Bij veel collega's ontbreken bovendien de vaardigheden om een dashboard te lezen, te begrijpen en te gebruiken.

Wat willen we bereiken?
De komende jaren zetten we verdere stappen om te groeien in volwassenheid als het gaat om informatiegestuurd werken. Informatiegestuurd werken wordt onderdeel van ons dagelijks werk. We ontwikkelen een centrale visie en integrale aanpak. Hierbij kijken we naar de mens (bewustwording, capaciteit, competenties) en naar de techniek (tooling, ontsluiting). Daarbij zoeken we ruimte om te experimenteren, waarbij we oog houden voor ethiek en privacy.
Dankzij nieuwe technieken en de beschikbaarheid van een grote hoeveelheid data uit eigen bronnen, openbare registers, sociale media en/of slimme analyses zijn we in staat om real time managementinformatie te genereren. Voor het nemen van beslissingen op basis van deze data is betrouwbaarheid en goede analyse van gegevens essentieel. Om onze ambities waar te kunnen maken creëren we inzicht in de huidige kwaliteit van onze data en vergroten we de datakwaliteit waar nodig.

Wat gaan we daarvoor doen?
- Een visie vaststellen op informatiegestuurd werken. Daaraan vooorafgaand voeren we een volwassenheidsmeting uit op het gebied van informatiegestuurd werken. Aan de hands daarvan stellen we vast waar we nu staan en wat onze ambities zijn;
- Verhogen datakwaliteit door processen te optimaliseren en te automatiseren. Daarnaast het koppelen
- van de verschillende bronnen, zodat je maar op 1 plek gegevens hoeft te registreren.
- Aan de hand van onze visie en ambities werken we aan een routekaart die ons gestructureerd langs verschillende sporen naar een hogere volwassenheid leidt.
- Een ethisch normenkader ontwikkelen en een wegingskader voor privacyvraagstukken
- bij het verwerken, gebruiken en delen van data.
- Doorontwikkelen van managementrapportages (dashboards).

Meer detailinformatie over de invulling van Informatiegestuurd werken lees je in het adviesrapport over Data Life Cycle management en de onderliggende beleidsstukken over o.a. bewaartermijnen, informatieclassificatie en datatoegangsbeleid. Deze zijn opgenomen in de bijlagen.

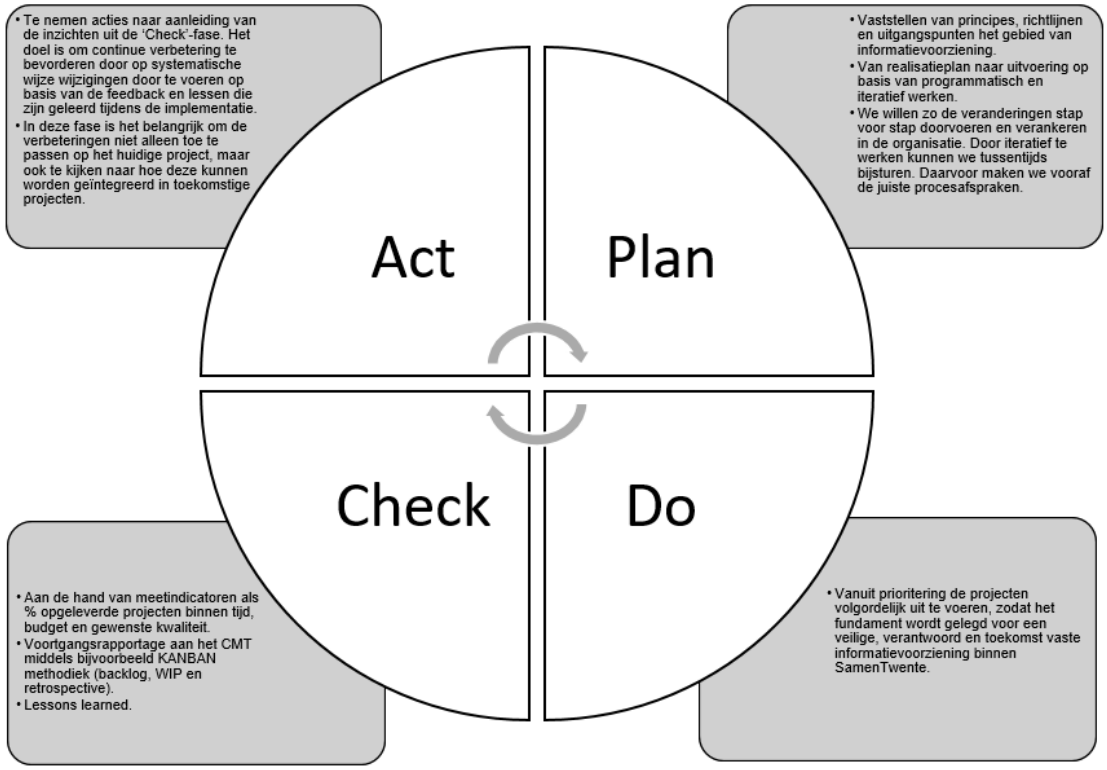
3 Borging informatiebeleid

In dit informatiebeleid staan verschillende ambities en opgaven voor de periode 2024 – 2028. Deze opgaven zijn vertaald naar concrete projecten in de projectenkalender. Na het vaststellen van de koers en ambitie is het belangrijk om het informatiebeleid structureel te borgen binnen de organisatie. We adviseren dit te doen langs twee lijnen: het projectportfolio en vertaling van de koers.

3.1 Projectportfolio

We weten nu nog niet wat er over vier jaar op ons af komt. Dit vraagt om een flexibiliteit en wendbaarheid bij het uitvoeren van het plan. Het is belangrijk om continu de voortgang te blijven meten om focus te houden op de kwaliteit van de uitvoering. Daarom adviseren we om te werken met een organisatiebreed projectenportfolio met projecten met een IM & T component. Zo beheersen we risico's en ontstaat er grip op en afstemming over
de prioritering van projecten. Komende tijd onderzoeken we hoe we dit vorm kunnen geven.

Projectenkalender 2024 – 2025
De eerste versie van de projectenkalender voor 2024 – 2025 vind je in de bijlage van dit plan, inclusief een financiële vertaling. We adviseren om de voortgang van het beleid periodiek, bijvoorbeeld halfjaarlijks, met het CMT te delen aan de hand van het portfolio. Het CMT kan van daaruit sturen op de strategische koers, de prioritering van projecten en de bijbehorende capaciteit en middelen. We hanteren hierbij de Plan – Do – Check – Act-cirkel. Het bestuur kan
bijsturen aan de hand van de reguliere P&C-cyclus.



3.2 De uitwerking van de nieuwe koers

Het informatiebeleid heeft impact op de medewerkers en de manier van werken binnen de organisatie. Met dit beleid schakelen we naar de noodzakelijke hogere versnelling. Dit vraagt wel wat van de organisatie. Daarom adviseren wij om na vaststelling van de koers in gesprek te gaan met de teams over de uitwerking van deze koers. Vragen die hierbij centraal staan, zijn:

- Wat vraagt het van onze medewerkers?
- Wat vraagt het van het team?
- Wat vraagt het van de sturing en manier van leidinggeven?
- Wat vraagt het van de organisatie als geheel?

Verschillende invulling en behoeften
De invulling en behoeften kunnen per team verschillen. De koers kan vervolgens in samenspraak met de organisatie worden vertaald naar concrete impact op mensen, middelen en werkwijzen. Dit vraagt om een continu proces en structurele aandacht. Waarschijnlijk betrekken we de OR, team HR en team communicatie bij dit proces.

Een forse investering
Deze koers en ambitie zijn niet vrijblijvend. Het vraagt de komende jaren om een forse investering in kennis, kunde, capaciteit en middelen. Dit is noodzakelijk om bij te blijven, te voldoen aan bestaande en nieuwe wet- en regelgeving en mee te groeien met de verwachtingen van de samenleving. Ook voor team IM&T geldt dat er komende jaren geïnvesteerd moet worden in capaciteit en middelen om deze ambities waar te maken. Na vaststellen van de koers door het CMT werken we de impact op de organisatie en team IM&T nader uit.

4 Realisatie informatiebeleid: projectenkalender en formatie

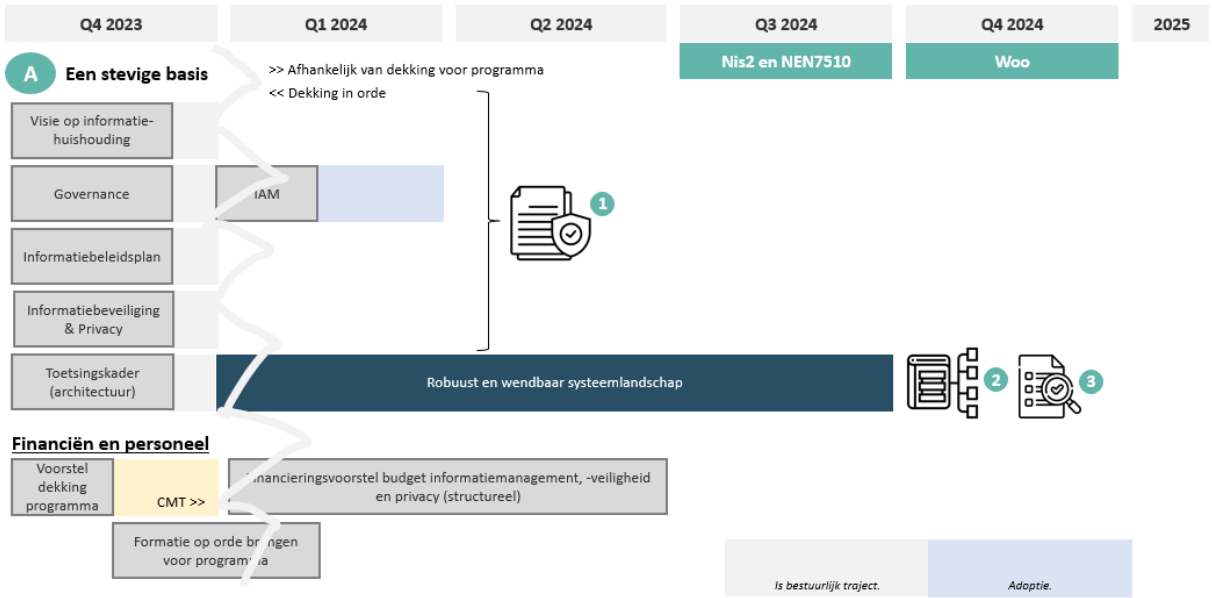
Het informatiebeleid zoals uitgewerkt in dit plan gaan we in de komende jaren realiseren. Om regie te houden op de realisatie van deze projecten en acties stellen we een projectenkalender op met daarbij een financiële vertaalslag. Bij de opstelling is rekening gehouden met:

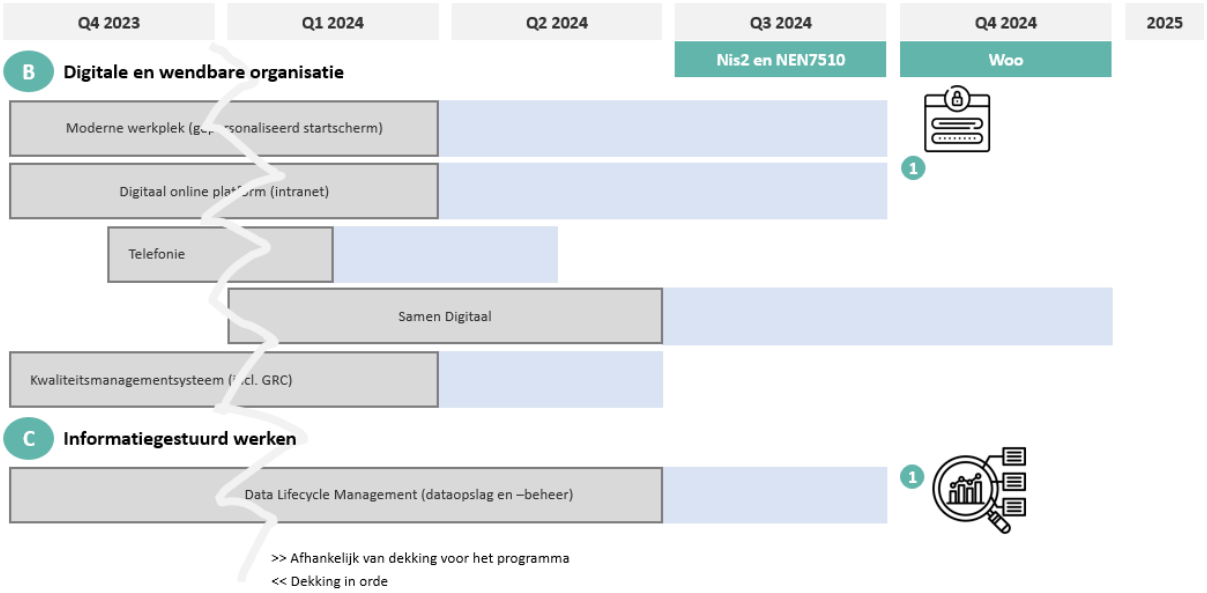
- wettelijke eisen en verplichtingen: wat moet er in die periode gerealiseerd zijn?
- reeds lopende projecten binnen SamenTwente
- capaciteit van het team IM&T en de organisatie
- beschikbare middelen

4.1 Kalender en financiële gevolgen

In bijlage 1 vind je de kalender, die is opgezet aan de hand van de sporen van het informatiebeleid. Voor de projecten en acties die in het uitvoeringsplan zijn opgenomen is een initiële raming gemaakt. Deze volgt in december 2023, maar in concept in november opgesteld en gebruikt voor een bestuursvoorstel over de structurele uitbreiding van personeel IM&T en IV&P.
Dit is een inschatting, bijvoorbeeld omdat er nog geen projectafspraken zijn gemaakt of omdat pas bij de definitieve afspraken en contracten met leveranciers volledige duidelijkheid is van de kosten. We moeten daarom rekening houden met een (on)nauwkeurigheidsfactor.

We willen realistisch begroten. Dit houdt in dat met name de raming voor 2024 meer detail bevat en nauwkeuriger is. De ramingen richting 2028 zijn minder nauwkeurig. Vandaar dat we ervoor kiezen om de projectenplanning jaarlijks te actualiseren en vast te stellen in het CMT met de route zoals voorgesteld in hoofdstuk 4. Voor de projecten en acties in 2024 voorzien we de volgende kosten per spoor:





4.2 Gevolgen voor personeel en formatie

We investeren niet alleen in de genoemde projectkosten: ook is het noodzakelijk om te investeren in formatie. Alleen zo kunnen we de uitgangspunten uit het informatiebeleidsplan realiseren. De huidige capaciteit binnen het team IM&T is onvoldoende om goed invulling te geven aan alle genoemde strategische opgaves. Voor 2024 en verder geldt dat er formatie nodig is voor de uitvoering van het Informatiebeleid, Informatiebeveiligingsbeleid en Privacybeleid.

Investeren in formatie
Op dit moment is de formatie binnen team IM&T erg fragiel. Het team beschikt formeel over 1 FTE informatieadviseur en 0,5 FTE Functionaris gegevensbescherming. Dat brengt de continuïteit van de informatievoorziening in gevaar. De capaciteitsbehoefte is nu opgevuld met een aantal informatiemanagers, een CISO en Privacy Officers die tijdelijk zijn ingehuurd. Voor deze tijdelijke formaties is geen structurele dekking. We financieren ze vanuit incidentele middelen. Het gaat hier echter wel om structurele lijnfuncties die tot de kern van de functies van IM&T behoren. De conclusie is dan ook, dat het team IM&T structureel onderbezet is. En dat is een risico voor SamenTwente. Het risico is, dat we onze ambities niet kunnen waarmaken en niet kunnen voldoen aan wette lijke verplichtingen. Deze constatering is gebaseerd op de huidige situatie over de informatiehuishouding: we hebben een bestuurlijk voorstel opgesteld dat in december met het Dagelijks en Algemeen Bestuur wordt besproken en daarna naar alle wethouders van de 14 gemeentes gaat met de juiste formatie binnen IM&T.

Investeren in kwaliteit
Ook is het nodig om te investeren in vaardigheden. Voor onze ambities op het gebied van informatiegestuurd werken hebben we namelijk ook een kwalitatieve achterstand. Op deze drie manieren kunnen we investeren in het verbeteren van de kwaliteit:
Nieuwe vaardigheden voor medewerkers in het IM&T-team. Want door de Woo krijgen informatiebeheerders veel meer een rol in het adviseren van afdelingen. Advies over het inrichten van de informatiehuishouding.

En advies over het doeltreffend en doelmatig vormgeven van:

- Het actief openbaar maken van informatie in de organisatie. Van oudsher is informatiebeheer immers vrij operationeel ingericht in organisaties.
- Verder vraagt informatiegestuurd werken om kennis en competenties op het gebied van datamanagement. Deze zijn nog niet aanwezig binnen SamenTwente.
- Normen als NEN7510 en NIS 2 moeten nog geïmplementeerd worden.

Samen Twente

Gezond, veilig vitaal

Informatiebeveiligings-beleid 2025-2028

Managementsamenvatting

Waarom dit informatiebeveiligingsbeleid?

- SamenTwente ondersteunt en versterkt de inzet en activiteiten van gemeenten en samenwerkingspartners om inwoners van Twente gezond, veilig en vitaal te houden. Hierbij werken we dagelijks met kritische, vertrouwelijke en persoonsgerelateerde informatie. Informatieveiligheid is daarom van het grootste belang voor de organisatie.
- Door technische ontwikkelingen neemt onze afhankelijkheid van informatie toe, en daarmee ook de noodzaak om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie zeker te stellen. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor burgers, bedrijven, partners en onze eigen organisatie. Ook heeft dit waarschijnlijk politieke consequenties en leidt het tot imagoschade.
- Dit vereist een integrale aanpak en voldoende risicobewustzijn, waar ieder organisatieonderdeel bij betrokken is. Verantwoord en bewust gedrag van medewerkers is essentieel om informatieveiligheid te bereiken en te behouden.

Toepassing informatiebeveiligingsbeleid in de praktijk:

- Dit informatiebeveiligingsbeleid beschrijft beleid op strategisch en organisatorisch niveau, en is richtinggevend en kaderstellend. Het vormt de basis voor een veilige informatievoorziening die zorgt voor een juiste balans tussen functionaliteit, veiligheid en privacy.
- Het beleid sluit aan bij de vitale missie van onze organisatie. Met dit beleid voeren we regie over informatieveiligheid, voldoen we aan de geldende wet- en regelgeving en kunnen we daar gepaste verantwoording over afleggen.
- Het informatiebeveiligingsbeleid sluit aan bij onze ambitie om de informatieveiligheid structureel naar een hoger niveau te brengen. Als de basis door implementatie van bijvoorbeeld de BIO en/of NEN7510 op orde is, verhoogt dit onze digitale weerbaarheid. Daarbij helpt deze regelgeving het lijnmanagement bij het nemen van zijn verantwoordelijkheid en het uitvoering geven aan informatiebeveiliging. De NIS2 richtlijn, gepland voor oktober 2024, zal dit uiteindelijk opnemen in de wet.

Versiebeheer

Versie	Datum	Door	Omschrijving
0.8	Jan 2018	H. van der Woning/ M.Kokhuis	Opmerkingen vanuit MT's RT verwerkt
1.0	07-02-2018	H. van der Woning	Versie 0.8 vastgesteld en opgewaardeerd naar versie 1.0
1.2		H. van der Woning	Aanpassingen n.a.v. evaluatie doorgevoerd
2.0	11-05-2021	H. van der Woning	Versie 1.2. vastgesteld door CMT en opgewaardeerd naar versie 2.0
2.1	Dec 2022	H. van der Woning	Versie 2.0 geactualiseerd naar SamenTwente
3.0	Jul 2023	H. Heerebout	Versie 3.0, SamenTwente versie voor CMT vaststelling
4.0	Nov. 2023	Olga Leever	Eindredactie versies 1, 2 en 3 door tekstschrijver
4.1	Nov 2024	G. Tijink	Laatste aanpassingen en updates ter vaststelling AB

Inhoudsopgave

1 Inleiding

Dit informatiebeveiligingsbeleid vormt de basis voor een veilige informatievoorziening die zorgt voor een juiste balans tussen functionaliteit, veiligheid en privacy. Het beleid sluit aan bij de vitale missie van onze organisatie.

Met dit beleid voeren we regie over informatieveiligheid, voldoen we aan de geldende wet- en regelgeving en kunnen we daar gepaste verantwoording over afleggen. Informatieveiligheid is een verantwoordelijkheid van al onze medewerkers. En dus is het van belang dat iedereen zich bewust is van ons informatiebeveiligingsbeleid.

Waarom een informatiebeveiligingsbeleid?
SamenTwente ondersteunt en versterkt de inzet en activiteiten van gemeenten en samenwerkingspartners om inwoners van Twente gezond, veilig en vitaal te houden. Hierbij werken we dagelijks met kritische, vertrouwelijke en vaak persoonsgerelateerde informatie. Informatieveiligheid is daarom van het grootste belang voor de organisatie.

Door technische ontwikkelingen neemt onze afhankelijkheid van informatie toe, en daarmee ook de noodzaak om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie zeker te stellen. Ook de samenleving stelt steeds hogere eisen aan de digitale volwassenheid en informatiebeveiliging van onze organisatie. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor burgers, bedrijven, partners en onze eigen organisatie. Ook heeft dit waarschijnlijk politieke consequenties en leidt het tot imagoschade.

Dit vereist een integrale aanpak en voldoende risicobewustzijn, waar ieder organisatieonderdeel bij betrokken is. Verantwoord en bewust gedrag van medewerkers is essentieel om informatieveiligheid te bereiken en te behouden.

Onze ambitie
SamenTwente heeft de ambitie om de informatieveiligheid structureel naar een hoger niveau te brengen. Als de basis door implementatie van bijvoorbeeld de BIO en/of NEN7510 op orde is, verhoogt dit onze digitale weerbaarheid. Daarbij helpt deze regelgeving het lijnmanagement bij het nemen van zijn verantwoordelijkheid en het uitvoering geven aan informatiebeveiliging. De NIS2 richtlijn, gepland voor oktober 2024, zal dit uiteindelijk opnemen in de wet.

Leeswijzer
Dit document beschrijft hoe we omgaan met informatiebeveiliging als onderdeel van het algemene en overkoepelende Informatiebeleid dat SamenTwente voert. Het beschrijft beleid op strategisch en organisatorisch niveau, en is richtinggevend en kaderstellend. Het beleid wordt aangevuld met per onderwerp specifieke beleidsregels, richtlijnen, standaarden en procedures.

2 Informatiebeveiligingsbeleid

Allereerst beschrijven we wat het doel, de randvoorwaarden en de uitgangspunten zijn van ons informatiebeveiligingsbeleid. Ook lees je in dit hoofdstuk hoe we omgaan met mogelijke ketenpartners en aan welke wetten en regels we ons moeten houden.

2.1 Doel informatiebeveiligingsbeleid

Informatiebeveiliging heeft tot doel de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen, en is zo gespecificeerd:

- Beschikbaarheid:
  De informatie is beschikbaar tijdens de bedrijfsvoering van de organisatie.
- Integriteit:
  De informatie is juist, volledig actueel, integer en gericht op de behoefte van de vrager.
- Vertrouwelijkheid:
  De informatie is alleen toegankelijk voor personen die vanuit hun rol/functie daar toegang tot mogen hebben.

Dit alles in ondersteuning bij het minimaliseren van beveiligings- en privacy incidenten, het nemen van mitigerende maatregelen en het verminderen van eventuele gevolgschade. Zie ook NORA kernwaarden van dienstverlening (kwd02)

2.2 Doelstellingen en randvoorwaarden

Om dit doel te kunnen bereiken, hebben we deze doelstellingen en gedefinieerd:

- De risico's beperken van misbruik, verlies, diefstal, fraude, uitval of beschadiging van informatiesystemen die SamenTwente gebruikt voor de verwerking van haar gegevens. Dit is met inbegrip van, maar niet beperkt tot, alle computers, netwerkapparatuur, software en hardware.
- Tijdig en zorgvuldig afhandelen van incidenten. En gepaste preventieve en corrigerende maatregelen nemen om risico op herhaling te beperken.
- Zorgen voor een veilige en betrouwbare werking van informatiesystemen. Daarbij maakt het niet uit of de systemen worden beheerd door ons of door daarvoor aangewezen leveranciers.
- Het beheer (de exploitatie) borgen van informatiesystemen om onbedoelde wijzigingen met mogelijke nieuwe risico's te voorkomen.
- Ons beschermen tegen aansprakelijkheid of schade door het misbruik van onze informatiesystemen en faciliteiten.
- Een kader bieden voor een adequate continuïteitstrategie. Met deze strategie beschermen we kritische bedrijfsprocessen tegen de gevolgen van uitval of onderbreking van informatiesystemen, of tegen het niet meer beschikbaar zijn van informatie. De strategie heeft ook als doel om hiervan continu te leren.
- Respecteren van de rechten van betrokkenen: cliënten, patiënten, medewerkers, bezoekers, leveranciers. Dit komt voort uit de AVG (Algemene Verordening Gegevensbescherming).
- Archiveren van de informatie van SamenTwente volgens de Archiefwet 1995, en vastgestelde bewaartermijnen.
- Voldoende informatiebeveiligingsbewustwording creëren bij alle interne en externe medewerkers.

Een randvoorwaarde is, dat Informatiebeveiliging, inclusief dit beleid, onderdeel uitmaakt van afspraken met ketenpartners en leveranciers die zorgdragen voor kritische bedrijfsonderdelen.

2.3 Reikwijdte

Dit beleid heeft betrekking op digitale middelen, software in eigendom of via licentie verkregen, gegevens en informatie, processen en onderliggende informatiesystemen binnen onze organisatie. Dit ongeacht locatie, tijdstip, vorm, toegangskanaal en gebruik van (privé) apparatuur van in- en externe werknemers voor de verwerking van gegevens van de organisatie. Alle gebruikers van diensten van SamenTwente, inclusief coalities en externe GR, moeten zich houden aan dit beleid.

2.4 Uitgangspunten

De voornaamste uitgangspunten van het informatiebeveiligingsbeleid zijn:

- Alle gegevens, informatie en informatiesystemen zijn van belang voor de organisatie. Bepaalde gegevens en systemen zijn zelfs van vitaal en kritiek belang.
- SamenTwente stelt de benodigde middelen beschikbaar om informatieveiligheid te borgen, en daarmee informatievoorziening en werkprocessen voldoende te beveiligen.
- Alle bedrijfsprocessen, informatiebronnen en -systemen die gebruikt worden voor de verwerking van gegevens bij SamenTwente hebben een verantwoordelijke eigenaar. Ze zijn geclassificeerd in relatie tot de bedrijfskritische waarde. Deze eigenaar is een interne medewerker op het niveau van teamleider of daarboven.
- Uitzonderingen op dit beleid worden vastgesteld, goedgekeurd en vastgelegd volgens het uitzonderingsproces.
- Elke medewerker is verplicht gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht. Vermoedt de medewerker inbreuken, dan is de medewerker verplicht hiervan melding te maken.
- Door periodieke controle en organisatiebrede planning en coördinatie wordt de kwaliteit van de informatievoorziening en -beveiliging verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan en -strategie het fundament onder een veilige informatievoorziening.
- In het informatiebeveiligingsplan en -strategie wordt de vertrouwelijkheid van de informatievoorziening organisatiebreed benaderd en uitgevoerd. Dit wordt elke twee tot drie jaar bijgesteld op basis van nieuwe ontwikkelingen, risico's of kennis.
- Bij verandering aan bestaande, of introductie van nieuwe informatiesystemen wordt informatiebeveiliging van begin af aan in de voorbereiding en uitvoering meegenomen.

2.5 Ketenpartners

Als we samenwerken met ketenpartners, wisselen we vertrouwelijke informatie uit en gebruiken deze informatie ook. Hierover leggen we afspraken vast in overeenstemming met ons beleid. Die afspraken gaan over verantwoordelijkheden, het treffen van passende beveiligingsmaatregelen en in te zetten middelen.

2.6 Normen, wet- & regelgeving

Met het opstellen van het informatiebeveiligingsbeleid voldoen we aan deze normen:

- NEN7510:2020:
  - Deel 1 (Medische informatica – Informatiebeveiliging in de zorg - Managementsysteem) en
  - Deel 2 (Medische informatica – Informatiebeveiliging in de zorg – Beheersmaatregelen).
- NEN-ISO_IEC 27017_2021 [Security controls for Cloud services]

Hierbij beschouwen we deze normen als aanvulling op de BIO (Baseline Informatiebeveiliging Overheid). De NIS2-richtlijnen, die van toepassing zijn voor vitale organisaties, verlangen daarnaast nog aanvullende maatregelen.

2.7 Niet-naleving

Naleving van dit beleid is vereist. Komen medewerkers het beleid niet na? En is daarbij sprake van opzet of bewuste roekeloosheid (art. 7:661 lid 1 BW) van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen? Dan beroepen wij ons op de aansprakelijkheid van de medewerker(s).

3 Organisatie van informatiebeveiliging

Wij houden ons aan het principe van 'scheiding van taken'. En dus worden rollen en verantwoordelijkheden centraal en decentraal belegd. Centraal bij onder meer informatiemanagement (IM) en ICT. En decentraal bij proceseigenaren en functioneel beheerders. Wat de bijbehorende actoren en verantwoordelijkheden zijn, lees je in dit hoofdstuk.

3.1 Dagelijks bestuur (DB): eindverantwoordelijke en kaderstellend

Het dagelijks bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen onze organisatie. Ook stelt het DB kaders op basis van de landelijke en Europese wet- en regelgeving en geldende normenkaders. Dit beleid is een verdere uitwerking van deze eindverantwoordelijkheid en bevoegdheid. Het bestuur stimuleert het CMT om passende maatregelen te treffen binnen deze vastgestelde kaders. Het dagelijks bestuur:

- stelt het beleid vast en draagt ervoor zorg dat wij aan de wettelijke eisen uit de BIO, NEN7510 en NIS2 voldoen
- stelt voldoende middelen beschikbaar om de informatiebeveiliging binnen SamenTwente te laten voldoen aan de gestelde eigen vereisten en wettelijke verplichtingen
- stelt voldoende middelen beschikbaar om informatiebewustzijn binnen de organisatie te borgen.

3.2 Directie en Management Team (CMT): vaststellen beleid

De directie en het CMT is verantwoordelijk voor het vaststellen van het beleid en de onderliggende richtlijnen voor adequate informatieveiligheid. Ook is het CMT verantwoordelijk voor het beoordelen van de efficiëntie en effectiviteit hiervan. Informatiebeveiliging valt binnen het CMT onder de manager bedrijfsvoering.

De directie en het CMT in het algemeen, en de manager bedrijfsvoering in het bijzonder, zijn eindverantwoordelijk voor de inrichting en werking van informatiebeveiliging en organisatie daarvan en:

- stuurt de organisatie op beveiligingsrisico's
- evalueert periodiek de beleidskaders en stelt waar nodig bij
- legt aantoonbaar verantwoording af over het gevoerde beleid.

3.3 Management Team (MT): leidinggeven aan de verschillende organisaties

Bedrijfsvoering, GGD Twente, Veilig Thuis Twente (VTT) en Organisatie voor Zorg en Jeugdhulp in Twente (OZJT) hebben elk een eigen MT. Deze MT's bestaan uit leidinggevenden van de verschillende organisaties. Het MT:

- valideert de afspraken rondom informatiebeveiliging op uitvoerbaarheid, zoals beschreven in beleid en richtlijnen
- controleert of de getroffen maatregelen overeenstemmen met de beveiligingseisen en of deze voldoende bescherming bieden
- wijst voor elk bedrijfsproces & informatiesysteem een proceseigenaar aan
- conformeert zich aan gevalideerd beleid

3.4 Proceseigenaren (Managers en leidinggevenden): dagelijkse verantwoording

De proceseigenaar (PE) is verantwoordelijk voor de integrale beveiliging van de bedrijfsprocessen en de daaraan gerelateerde informatiesystemen. Daarmee heeft hij/zij/hen de dagelijkse verantwoording.

De PE ziet voortdurend toe op naleving van de vastgestelde richtlijnen en beoordeelt de risico's en dreigingen. De proceseigenaar:

- bepaalt op basis van een expliciete risicoafweging de waarde en classificatie van het bedrijfsproces en daaraan gerelateerde informatiesystemen
- stelt de beveiligingseisen en voorwaarden vast voor het bedrijfsproces in lijn met het geldende beleid
- kiest op basis van deze beveiligingseisen de beveiligingsmaatregelen en draagt deze uit
- legt aantoonbaar verantwoording af over de beveiliging van het bedrijfsproces door objectieve meetgegevens
- stuurt beveiligingsbewustzijn, bedrijfscontinuïteit en de naleving van regels en richtlijnen aan
- meldt beveiligingsincidenten en rapporteert in hoeverre bedrijfsprocessen/informatiesystemen voldoen aan het informatiebeveiligingsbeleid.

Managers en leidinggevenden hebben daarnaast een voorbeeldfunctie als het gaat om informatiebeveiliging. Ze zijn proactief en signalerend, houden rekening met het beleid binnen de hele organisatie, stimuleren samenwerking en dragen bewustzijn uit naar de teams.

3.5 Bedrijfsvoering: verantwoordelijk voor de uitvoering

Voor de operationele bedrijfsvoering zijn diverse rollen en teams verantwoordelijk, zoals functioneel beheerders (FB), P&O (HRM), facilitair en IM&T. Zij zijn verantwoordelijk voor de uitvoering van:

- de beveiliging van de informatievoorziening en implementatie van maatregelen die voortvloeien uit de beveiligingseisen en bijbehorende risicoanalyses
- maatregelen gericht op beveiliging van personeel zoals screening en geheimhoudingsverklaringen
- het bijhouden en actualiseren van de functies, rollen en verantwoordelijkheden
- maatregelen gericht op (fysieke en logische) beveiliging van gebouwen, publieke en interne werkruimtes van SamenTwente
- het uitdragen en bewustwording van dit informatiebeveiligingsbeleid
- het ondersteunen van proceseigenaren en beheren van de operationele bedrijfsvoering van de gerelateerde informatiesystemen.

3.6 Informatiemanagement & Technologie (IM&T): beveiligingstaken

De trend van digitalisatie geeft de IM&T-organisatie een specifieke en breed gedragen informatiebeveiligingstaak, en is daarmee ook verantwoordelijk voor:

- alle beheeraspecten van informatiebeveiliging die betrekking hebben op ICT-aangelegenheden en digitale systemen. Denk hierbij aan incident- en probleemmanagement, configuratie- en wijzigingsbeheer, veilige bedrijfsvoering, logging van activiteiten en back-up & recovery
- het onderhouden van een eigen Plan van Aanpak (PvA), strategie en architectuur die overeenstemmen met het informatiebeveiligingsbeleid van de organisatie
- opstellen van procedures en werkinstructies ter ondersteuning van het te voeren informatiebeveiligingsbeleid
- verbeteringen aandragen voor het informatiebeveiligingsbeleid

3.7 Chief Information Security Officer (CISO): toezichthouden en toetsen

De CISO heeft een toezichthoudende en toetsende rol. Deze functie is belegd bij informatiemanagement & Technologie (IM&T). De CISO ondersteunt bestuur en CMT door coördinerende en adviserende taken die voortkomen uit het informatiebeveiligingsbeleid. Dit zijn de taken van de CISO:

- verantwoordelijk voor beleidsvorming, controle en registratie, communicatie en voorlichting over en realisatie van informatiebeveiliging voor de organisatie
- jaarlijks een herziening uitvoeren op alle beleidsonderdelen, en zorgen voor doorlopende aansluiting van het beleid en strategie van de organisatie
- controleren van de werking en de naleving van het Informatiebeveiligingsbeleid en daaruit voortvloeiende maatregelen. Ook het uitvoeren van audits en analyses hoor hierbij
- ontwikkelingen bijhouden op het gebied van informatiebeveiliging en dit vertalen naar oplossingen voor de organisatie
- adviseren over informatiebeveiligingsbeleid, verbetervoorstellen opstellen voor de informatiebeveiliging in een PvA en passende maatregelen nemen bij beveiligingsincidenten
- het managementsysteem voor informatiebeveiliging (ISMS) onderhouden, inclusief periodieke rapportage
- centraal aanspreekpunt van de organisatie voor informatiebeveiliging en de bewaking van risico's
- coördineren en adviseren bij informatiebeveiligingsincidenten, en verantwoordelijk voor rapportages
- faciliteren en adviseren van de proceseigenaren en functioneel beheerders bij het implementeren van beveiligingsmaatregelen
- verantwoordelijk voor verder professionaliseren van het periodieke informatiebeveiliging-verantwoordingsproces (P&C-cyclus)

3.8 Information Security Officer (ISO): adviseren over informatiebeveiliging

De ISO, ook wel adviseur informatiebeveiliging, valt onder Informatiemanagement & Technologie (IM&T):

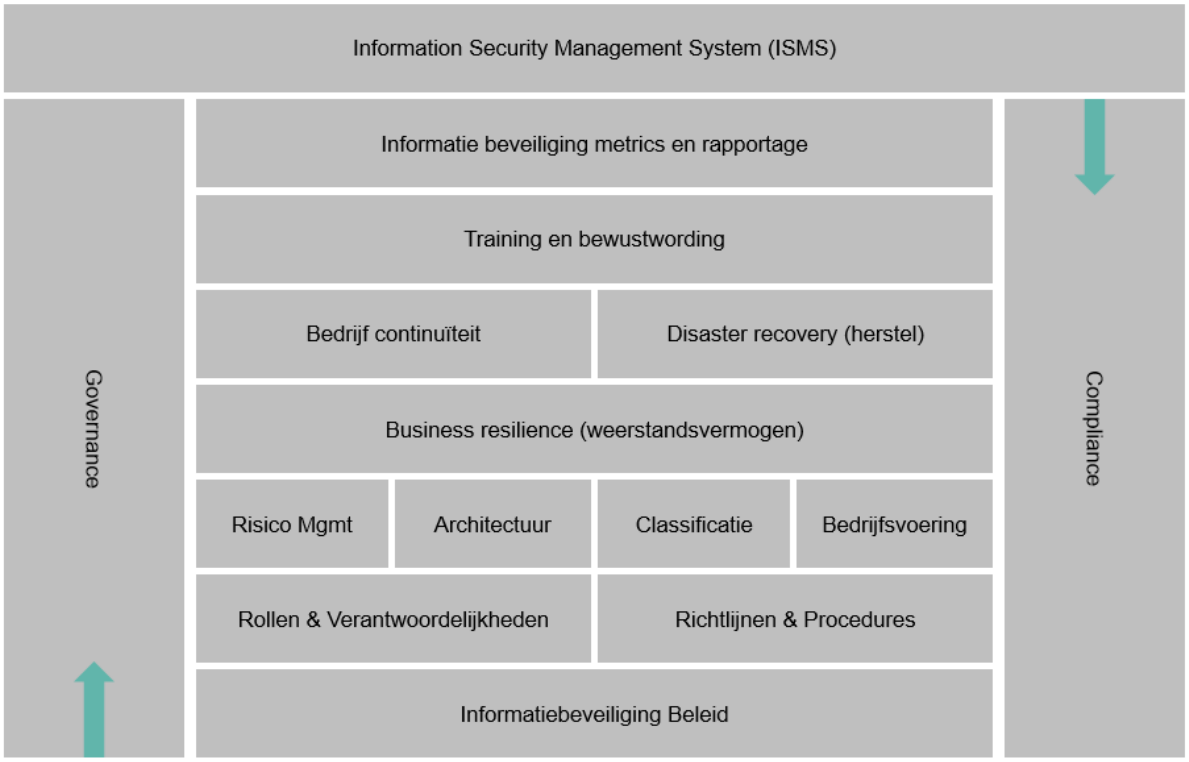
- adviseert de organisatie over de informatiebeveiliging op tactisch en operationeel niveau, in samenwerking met de functionaris gegevensbescherming (FG) en de CISO.
- is verantwoordelijk voor het opstellen van het Informatiebeveiligingsbeleid en voert regie op de uitvoering hiervan binnen de organisatie.
- adviseert bij besluitvorming over gevolgen voor informatiebeveiliging
- draagt actief uitvoeringsrichtlijnen op het gebied van informatiebeveiliging uit
- voert beveiligingsrisicoanalyses uit op technisch, proces- en businessniveau.

3.9 Medewerkers: verantwoordelijk op individueel niveau

Informatiebeveiliging is een gedeelde verantwoording. Elke interne of externe medewerker is verantwoordelijk voor informatiebeveiliging. Op individueel niveau is hij/zij/hen verantwoordelijk voor een effectieve informatiebeveiliging van de gegevens waar hij/zij/hen mee werkt.. Ook wordt van elke medewerker verwacht dat hij/zij/hen eventuele beveiligingsincidenten tijdig meldt in het daarvoor bestemde registratiesysteem.

4 Controle en verantwoording

Informatiebeveiliging en de naleving ervan zijn procesmatig ingericht via een Information Security Management System (ISMS). Besteden we diensten uit, dan is Informatiebeveiliging onderdeel van al onze processen en contracten. Daarmee is Informatiebeveiliging geborgd en onderdeel van onze bedrijfs- en kwaliteitscyclus.



Afbeelding 1 ISMS

4.1 Het informatiebeveiligingsplan

Jaarlijks stelt de CISO een informatiebeveiligingsplan op, ook wel plan van aanpak (PvA) genoemd. Dit plan wordt voorgelegd aan de verschillende MT's voor afstemming en toetsing op uitvoerbaarheid. Na akkoord van de MT's gaan we over tot de implementatie door de verschillende teams/afdelingen. De resultaten ervan worden gerapporteerd aan het CMT, geëvalueerd en waar nodig vertaald naar een nieuwe of aangepaste strategie en PvA. Deze methode volgt het principe van Plan, Do, Check en Act (PDCA).

Zo meten we de resultaten

De feitelijke werking van de vastgestelde beveiligingsmaatregelen wordt door IM&T jaarlijks geactualiseerd via interne of externe controles, aangevuld met meetgegevens als steekproeven en (penetratie)testen. Dit valt onder de verantwoordelijkheid van CISO. Daarnaast test IM&T vaardigheden en operationele procedures periodiek op volledigheid en betrouwbaarheid. De CISO rapporteert deze uitkomsten met eventuele verbetervoorstellen aan het MT en het bestuur.

BIJLAGE 1 – Ondersteunende documenten

In deze bijlage vind je een globaal overzicht van de documenten waarin uitvoering van het informatiebeveiligingsbeleid SamenTwente verder is uitgewerkt. Deze en overige aan informatiebeveiliging gerelateerde documenten zijn ook opgenomen in het kwaliteitsbeheersysteem.

- *'Personeelshandboek SamenTwente'*
  In het Personeelshandboek SamenTwente (specifiek artikel 22.5/22.6) is vastgelegd hoe medewerkers met elektronische communicatiemiddelen moeten om gaan.

- *'Gedragscode SamenTwente'*
  In de Gedragscode 2021 en de Gedragscode Toelichting 2021 zijn gedragsnormen opgenomen voor het omgaan met vertrouwelijke informatie.

- *'Integriteitsbeleid SamenTwente'*
  In het Integriteitsbeleid SamenTwente 2009_2021 staan beleidsregels die o.a. aangeven hoe de medewerkers van ST behoren om te gaan met internet en e-mail.

- *'Privacybeleid SamenTwente'*
  In het Privacybeleid SamenTwente staan beleidsregels die aangeven hoe de medewerkers van ST behoren om te gaan met persoonsgegevens.
  In dit beleid wordt een vertaalslag gemaakt van de verplichtingen uit de Algemene Verordening Gegevensverwerking (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) en wordt omschreven hoe SamenTwente invulling geeft aan het wettelijk kader.

- *'Privacyreglement GGD Twente'*
  In het Privacyreglement GGD Twente is vastgelegd welke regels en gedragscodes van toepassing zijn op het verkrijgen, bewerken of verwerken van persoonsgegevens door GGD-medewerkers in verband met het uitoefenen van hun functie. Daarnaast worden de rechten van cliënten en/of patiënten over hun vastgelegde persoonlijke gegevens beschreven. In het document Privacyreglement GGD Twente – Toelichting wordt een toelichting gegeven op het Privacyreglement.

- *'Informatiebeveiligingsbeleid Regio Twente'*
  Dat is het document dat je nu voor je hebt.

- *'Beleid en werkwijze uitwisselen privacygevoelige en vertrouwelijke informatie'*
  Het document 'Beleid en werkwijze uitwisselen privacygevoelige en vertrouwelijke informatie' beschrijft richtlijnen voor de beschikbare en toegestane tooling voor het veilig uitwisselen van informatie.

- 'Procedure *afhandeling datalekken Regio Twente'*
  In het document Procedure afhandeling datalekken Regio Twente is de procedure vastgesteld voor het gestructureerd afhandelen van beveiligingsincidenten die kunnen leiden tot een datalek. Deze procedure is opgenomen in een PDCA-cyclus om actualiteit en kwaliteit van de procedure te kunnen borgen.

BIJLAGE 2 – Afkortingen

ISMS	Information Security Management System. Beschrijft de beleidsuitgangspunten en uitvoering daarvan voor informatiebeveiliging. Het beschrijft onder andere de risico-analysemethodiek die een organisatie hanteert en de daarop genomen maatregelen voor borging van informatieveiligheid volgens de PDCA-cyclus.
NEN7510	De door het Nederlands Normalisatie-instituut, ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland gebaseerd op de ISO standaarden 27001 en 27002.
NEN7512	De norm NEN 7512 is een verdere specificatie van NEN7510 en richt zich op de 'vertrouwensbasis voor gegevensuitwisseling' tussen partijen.
NEN7513	De norm NEN 7513 is een verdere specificatie van NEN7510 en richt zich op 'Logging' van acties op het elektronisch patiëntendossier, zodat achterhaald kan worden wie er toegang heeft gehad tot het dossier.
NEN-ISO_IEC 27017_2021 [Security controls for Cloud services]	NEN-EN-ISO/IEC 27017 geeft richtlijnen voor informatiebeveiligingscontroles die van toepassing zijn op de levering en het gebruik van clouddiensten door het verstrekken van: - aanvullende implementatierichtlijnen voor relevante controles gespecificeerd in ISO / IEC 27002 - aanvullende controles met implementatierichtlijnen die specifiek betrekking hebben op cloudservices Deze aanbeveling | International Standard biedt controles en implementatierichtlijnen voor zowel cloudservice providers als cloudservice klanten.
PDCA	(Plan – do –check – Act): managementmethode voor continue proces- en productoptimalisatie en -verbetering.
PO	Privacy Officer
GR	Gemeenschappelijke Regeling
SamenTwente	SamenTwente is de overkoepelende organisatie voor de organisaties GGD Twente, Veilig Thuis Twente (VTT) en Organisatie voor Zorg en Jeugdhulp in Twente (OZJT) en voor de coalities Twentse Koers, Samen14 en Kennispunt Twente.

Samen Twente

Gezond, veilig x3 vitaal

Privacybeleid 2025-2028

Managementsamenvatting

Waarom een privacybeleid?

- De maatschappij is gedigitaliseerd en ook de overheid werkt steeds digitaler. Samen met de snelle technologische ontwikkelingen en globalisering brengt dit nieuwe uitdagingen voor de bescherming van persoonsgegevens met zich mee.
- Een privacybeleid is nodig omdat SamenTwente veel persoonsgegevens verwerkt. Het is belangrijk voor ons om deze gegevens op de juiste wijze te verwerken en beschermen. Ook als we deze gegevens delen met ketenpartners of andere derden. We willen immers voorkomen dat deze gegevens in verkeerde handen terechtkomen, waardoor er misbruik van kan worden gemaakt.
- We willen onze governance goed op orde hebben. Onder governance verstaan we het goed, efficiënt en verantwoord leiden van een organisatie. Daarvoor is het belangrijk om de rollen en verantwoordelijkheden helder te hebben. We beschrijven ze dan ook in dit privacybeleid. Hierdoor kunnen we de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd uitvoeren. Zo borgen we de privacy binnen SamenTwente en waarborgen we de rechten van alle betrokkenen.

Wat willen we met dit privacybeleid bereiken?

- Het is noodzakelijk een privacybeleid vast te stellen volgens nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG). Ook leggen we in dit beleid vast hoe we hier invulling aan geven.
- Het beleid is een uitgangspunt in onze processen, werkinstructies en richtlijnen.
- We leggen hiermee de kwaliteit van de verwerking en de beveiliging van persoonsgegevens vast en optimaliseren deze.
- Het biedt ons een kader om tot verbeterde compliance te komen. Het privacybeleid maakt het mogelijk (toekomstige) verwerkingen van persoonsgegevens te toetsen aan relevante wet- en regelgeving. Het is een vastgestelde 'best practice' of norm en helpt ons om de taken, bevoegdheden en verantwoordelijkheden in de organisatie vast te leggen.
- Met dit beleid dragen we bij aan bewustzijn (awareness) over het belang en de noodzaak van het beschermen van persoonsgegevens bij interne en externe medewerkers. Als medewerkers zich hiervan bewust zijn, zijn ze gemotiveerd en zien ze het belang om het privacybeleid van SamenTwente goed uit te voeren.

Versiebeheer Privacybeleid SamenTwente 2025-2028

Versie	Datum	Auteurs	Opmerkingen
1.0	15-11-2024	Team Privacy	Vastgesteld door Dagelijks Bestuur

Inhoudsopgave

1 Inleiding

Met dit privacybeleid wil SamenTwente de kwaliteit van de verwerking en de beveiliging van persoonsgegevens vastleggen en optimaliseren. Ook leggen we hierin vast hoe we invulling geven aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG). Dit privacybeleid gebruiken we als uitgangspunt in onze processen, werkinstructies en richtlijnen.

Waarom is dit nodig?
De maatschappij is gedigitaliseerd en ook de overheid werkt steeds digitaler. Samen met de snelle technologische ontwikkelingen en globalisering brengt dit nieuwe uitdagingen voor de bescherming van persoonsgegevens met zich mee. Het is daarom noodzaak om zorgvuldig om te gaan met persoonsgegevens. Misbruik kan immers grote schade toebrengen aan de betrokkenen.

Een privacybeleid is noodzakelijk omdat SamenTwente veel gegevens verwerkt. De meeste daarvan zijn persoonsgegevens. Voor ons is het belangrijk om de persoonsgegevens die aan ons worden verstrekt op de juiste wijze te verwerken en beschermen.

1.1 Doelstellingen privacybeleid

Concreet zijn dit de doelstellingen van ons privacybeleid:

- Een **kader** bieden om tot verbeterde compliance te komen. Het privacybeleid maakt het mogelijk (toekomstige) verwerkingen van persoonsgegevens te toetsen aan relevante wet- en regelgeving. Het is een vastgestelde 'best practice' of norm en helpt ons om de taken, bevoegdheden en verantwoordelijkheden in de organisatie vast te leggen.
- Ook dragen we met dit beleid bij aan **bewustzijn** (awareness) over het belang en de noodzaak van het beschermen van persoonsgegevens bij interne en externe medewerkers. We willen dat medewerkers het privacybeleid en daarmee de standpunten van SamenTwente kennen en weten wat er van hen wordt verwacht.

Dit realiseren we door onder meer:

- **Normen** te stellen en maatregelen te nemen. Het privacybeleid en het informatiebeveiligingsbeleid vormen de basis voor de bescherming en beveiliging van persoonsgegevens van SamenTwente.
- **Verantwoordelijkheid** te nemen. Directeur, managers en alle interne en externe medewerkers nemen verantwoordelijkheid in de verwerking van persoonsgegevens.
- Daadkrachtige **communicatie** over het privacybeleid binnen SamenTwente. Iedere medewerker, zowel intern als extern, is op de hoogte van het privacybeleid.

1.2 Reikwijdte privacybeleid en samenhang met overig beleid

Het privacybeleid heeft betrekking op het verwerken van persoonsgegevens van betrokkenen binnen (de systemen van) SamenTwente. Dit zijn in ieder geval inwoners van Twente, medewerkers en externe relaties. We willen de rechten en vrijheden van deze mensen adequaat waarborgen.

Het privacybeleid is een intern stuk dat het dagelijks bestuur van SamenTwente vaststelt, op advies van de Functionaris Gegevensbescherming. Het privacybeleid werken we uit in processen, werkinstructies, richtlijnen, overeenkomsten, privacyverklaringen en zo nodig andere stukken die informatie bieden over de verwerking van persoonsgegevens binnen SamenTwente. De toepassing van het beleid wordt jaarlijks getoetst. Als het nodig is, passen we dit beleid aan.

Relaties met andere beleidsterreinen
Bij SamenTwente wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met informatiebeveiliging. Daarbij gaat het om de beschikbaarheid, integriteit en vertrouwelijkheid van data, waaronder persoonsgegevens.

Ook is er een belangrijke relatie met het omgaan met data en daaruit gegenereerde informatie. Op strategisch niveau schenken we aandacht aan deze en andere raakvlakken en zoeken we planmatig en inhoudelijk afstemming met de juiste vakgroepen en functionarissen, zoals de CISO en de CIO.

1.3 Indeling en AVG-rollen SamenTwente
SamenTwente bestaat uit GGD Twente, Veilig Thuis Twente (VTT) en Organisatie voor Zorg en Jeugd in Twente (OZJT). Daarnaast is SamenTwente gastheer van de samenwerkingen Samen14, Kennispunt Twente en Twentse Koers. Al deze entiteiten zetten zich in voor een gezond, veilig en vitaal Twente. Het privacybeleid geldt voor al deze entiteiten.

Verschillen in entiteiten
Een groot verschil tussen deze entiteiten is de kwalificatie in het kader van de AVG. Deze verschilt per situatie in de praktijk. Bij ieder project en iedere verwerking die wordt gestart, wordt bepaald wat de kwalificatie van SamenTwente voor die verwerking is en welke maatregelen daarbij nodig zijn.

AVG-rollen
GGD Twente, VTT en OZJT zijn in bijna alle gevallen verwerkingsverantwoordelijke, bij het uitvoeren van een eigen wettelijke taak of een door de gemeenten overgedragen wettelijke taak. Bij samenwerking bijvoorbeeld met andere GGD'en of Veilig Thuis-organisaties kan er ook sprake zijn van gezamenlijke verwerkingsverantwoordelijkheid. Soms treden GGD Twente, VTT en OZJT op als verwerker, afhankelijk van de opdracht van de gemeenten.

Voor **Samen14, Kennispunt Twente en Twentse Koers** kwalificeert SamenTwente als verwerker, door het technisch beschikbaar stellen van zijn infrastructuur waaronder zijn Microsoft 365-omgeving. De deelnemers aan deze gastorganisaties zijn zelf (gezamenlijk) verwerkingsverantwoordelijk voor (de omgang met) de databestanden en de gebruikte technische oplossingen. Zij zijn aan het privacybeleid van SamenTwente gebonden als en voor zover deze de bescherming van persoonsgegevens door SamenTwente raken.

2 Juridisch kader en beleidskader

In dit hoofdstuk lees je aan de hand van welke wet- en regelgeving wij dit privacybeleid hebben opgesteld. Ook beschrijven we de uitgangspunten van het beleid en de beginselen waaraan de verwerking van persoonsgegevens moet voldoen. In de bijlage vind je een begrippenlijst.

2.1 Wet- en regelgeving
Wij hebben dit privacybeleid opgesteld volgens de daarvoor geldende wet- en regelgeving.
Privacywetgeving die voor SamenTwente altijd relevant is:

- Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG)
- Telecommunicatiewet (TW)
- Wet open overheid, Archiefwet 1995 en Wet digitale overheid

Er is nog meer privacy gerelateerde wet- en regelgeving van toepassing. Dit is afhankelijk van de werkzaamheden en is daarnaast sectorspecifiek. Daarbij gaat het om:

- Wet publieke gezondheid (Wpg), Besluit publieke gezondheid (Bpg) en Regeling publieke gezondheid
- Wet op de geneeskundige behandelingsovereenkomst (Wgbo) en Wet op de beroepen in de individuele gezondheidszorg (Wet BIG)
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en Besluit elektronische gegevensverwerking door zorgaanbieders
- Wet algemene bepalingen burgerservicenummer (Wab bsn), Besluit gebruik bsn in de zorg en Regeling gebruik bsn in de zorg
- Wet elektronische gegevensuitwisseling in de zorg (Wegiz)
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz) en Uitvoeringsbesluit Wkkgz
- Geneesmiddelenwet
- Vreemdelingenwet 2000 en Vreemdelingenbesluit 2000
- Wet maatschappelijke ondersteuning 2015 (Wmo 2015), Uitvoeringsbesluit Wmo 2015 en Uitvoeringsregeling Wmo 2015
- Jeugdwet, Besluit Jeugdwet, Regeling Jeugdwet, Regeling justitiële keteninformatisering Jeugdwet
- Burgerlijk Wetboek Boek 7 Titel 10 (arbeidsovereenkomst)

De wet- en regelgeving die van toepassing is, is aangevuld met talrijke richtlijnen, protocollen, veldnormen en jurisprudentie. In dit privacybeleid volstaan wij ermee te attenderen op deze aanvullende normen.

2.2 Beleidsuitgangspunten

Algemeen beleidsuitgangspunt is:

- Wij verwerken persoonsgegevens in overeenstemming met de relevante wet-en regelgeving, op behoorlijke en zorgvuldige wijze en transparant richting betrokkenen.
- Als de belangen van de betrokkene in strijd zijn met de belangen van de organisatie vindt een zorgvuldige belangenafweging plaats.

Om aan dit beleidsuitgangspunt te voldoen, voldoet, conform de AVG, elke verwerking van persoonsgegevens aan de volgende beginselen.

2.2.1 Rechtmatigheid

Elke verwerking van persoonsgegevens binnen SamenTwente baseren wij op een van de wettelijke grondslagen zoals genoemd in artikel 6 AVG. Het verwerken van bijzondere persoonsgegevens is in beginsel verboden. Dit doen wij dan ook uitsluitend als bovendien ten minste één van de uitzonderingsgronden van artikel 9 lid 2 AVG van toepassing is.
Als er geen andere grondslag zoals bedoeld in artikel 6 en/of artikel 9 lid 2 AVG is, dan verwerken wij persoonsgegevens alleen als de betrokkene hiervoor (uitdrukkelijk en expliciet) toestemming heeft gegeven. Bij alle registraties die gebaseerd zijn op de toestemmingen van de betrokkenen is het intrekken van de toestemming even eenvoudig als het geven van toestemming.

2.2.2 Behoorlijkheid en transparantie

We verwerken persoonsgegevens alleen op een manier die voor de betrokkene behoorlijk en transparant is. We kunnen ons op elk moment verantwoorden over de inrichting van de verwerkingen. Wij maken voor betrokkenen inzichtelijk in hoeverre en op welke manier wij persoonsgegevens verwerken en wij informeren betrokkenen onder andere in privacyverklaringen.

2.2.3 Doelbinding

Persoonsgegevens verwerken wij alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden leggen wij voor de start van de verwerkingsactiviteit vast. Wij verwerken persoonsgegevens niet verder op een wijze die onverenigbaar is met de doelen waarvoor wij deze oorspronkelijk hebben ontvangen.
Wij delen persoonsgegevens, zowel intern als extern, alleen als dat strikt noodzakelijk is voor het doeleinde van de verwerking en alleen met diegene die rechtstreeks betrokken is. Daarbij nemen wij de grootste zorgvuldigheid en terughoudendheid in acht als wij persoonsgegevens aan derden verstrekken.

2.2.4 Dataminimalisatie

Als wij persoonsgegevens verwerken, blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De persoonsgegevens zijn toereikend, ter zake dienend, en niet bovenmatig. Anders verwerken wij geen persoonsgegevens. De gegevensverwerking is proportioneel. Dat betekent dat deze in redelijke verhouding staat tot het beoogde doel. De gegevensverwerking is ook subsidiair. Dat houdt in, dat deze op de minst ingrijpende wijze gebeurt en dat wij die niet op een andere manier kunnen verwezenlijken die voor de betrokkenen minder nadelig is (proportionaliteit en subsidiariteit).

2.2.5 Juistheid

Wij treffen maatregelen om zoveel mogelijk te waarborgen dat de persoonsgegevens die wij verwerken juist en actueel zijn. Het up-to-date houden van de persoonsgegevens is hierbij relevant.

2.2.6 Beschikbaarheid, integriteit en vertrouwelijkheid

Wij beveiligen persoonsgegevens adequaat volgens de geldende beveiligingsnormen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid.
Daarnaast nemen wij gepaste organisatorische maatregelen om persoonsgegevens te beschermen. Zo laten wij persoonsgegevens niet onbeheerd en in open zicht achter. Ook hebben wij voor het verwerken van persoonsgegevens werkwijzen vastgesteld en voeren wij de verwerking op professionele wijze uit.

2.2.7 Opslagbeperking

Wij bewaren persoonsgegevens niet langer dan noodzakelijk is voor de doelen waarvoor ze zijn verzameld. Hierbij nemen wij de bewaar- en vernietigingstermijnen in acht die van toepassing zijn. Per verwerking stellen wij een bewaar- en/of vernietigingstermijn vast.
Als het voor een specifieke toepassing niet noodzakelijk is om persoonsgegevens te herleiden tot het individu, verwijderen wij deze persoonsgegevens en/of anonimiseren wij gegevens.

2.2.8 Privacy by design en Privacy by default

Als wij systemen, werkprocessen en/of diensten inrichten, gaan wij uit van de principes Privacy by Design en Privacy by Default.
Wij beschermen de privacy gedurende de hele levenscyclus van de gegevens van de betrokkenen (ontvangen gegevens, uitvoeren taak of overeenkomst en bewaken gegevens, bewaren gegevens, vernietigen gegevens).

2.2.9 Rechten van betrokkene

Iedere betrokkene heeft het recht om zijn rechten zoals bedoeld in hoofdstuk 7 uit te oefenen. Dat is bijvoorbeeld het recht op inzage of verwijdering van de persoonsgegevens die wij verwerken.
Wij handelen klachten en bezwaarschriften over privacyaspecten af en wij stellen de procedure voor behandeling van AVG-verzoeken vast door of met bindend advies van de Functionaris Gegevensbescherming op een toegankelijke, laagdrempelige wijze.

2.2.10 Datalekken
Wij melden inbreuken op persoonsgegevens altijd aan het privacy team van SamenTwente. Het is medewerkers niet toegestaan om zelfstandig datalekken te melden bij de Autoriteit Persoonsgegevens.

2.2.11 Awareness
Wij werken intern aan awareness van privacy, gegevensbescherming en informatiebeveiliging.

2.2.12 Naleving en toezicht
De directeur en het management dragen het privacybeleid uit binnen de organisatie. De Functionaris Gegevensbescherming houdt intern toezicht op de naleving en stelt de directeur op de hoogte als blijkt dat wij het privacybeleid niet op een juiste wijze uitvoeren.

3 De gegevensverwerking

In dit hoofdstuk beschrijven we met welke persoonsgegevens wij te maken krijgen en hoe we deze verwerken. Ook lees je welke doeleinden de gegevensverwerking heeft en welke werkprocessen we hanteren.

3.1 Aard en omvang persoonsgegevens
Bij het uitvoeren van taken verwerken wij verschillende soorten persoonsgegevens. Voorbeelden zijn cliëntgegevens, het behandelen van bezwaren of klachten en verwerkingen vanuit werkgeverschap. Regelmatig delen wij persoonsgegevens met ketenpartners of andere derden. Dit is bijvoorbe eld het geval als wij een verwerker inschakelen of als we werknemersgegevens aan de Belastingdienst moeten verstrekken.

Wij verwerken alle mogelijke categorieën van persoonsgegevens, waaronder gewone persoonsgegevens met een gevoelig karakter en bijzondere persoonsgegevens. Onze verwerkingen hebben we opgenomen in een verwerkingsregister. Daarin geven wij van iedere afzonderlijke verwerking nadere informatie over onder meer:

- de verwerkingsdoeleinden
- de categorieën betrokkenen
- de categorieën persoonsgegevens
- de categorieën ontvangers
- de grondslag van de verwerking
- de herkomst van de persoonsgegevens
- de bewaartermijn van de persoonsgegevens
- de beveiligingsmaatregelen

Het verwerkingsregister is beschikbaar bij de Privacy Officer en de Functionaris Gegevensbescherming en is toegankelijk voor alle proceseigenaren. De verwerkingen die wij uitvoeren, zijn beschreven in de privacyverklaringen van SamenTwente.

3.1.1 Gewone persoonsgegevens
Wij verwerken bij onze werkzaamheden allerlei categorieën persoonsgegevens. De persoonsgegevens zijn bijvoorbeeld:

- persoonlijke identificatiegegevens
- persoonlijke kenmerkgegevens
- werk gerelateerde gegevens
- contactgegevens

Gewone persoonsgegevens met een gevoelig karakter
Daarnaast verwerken wij persoonsgegevens met een gevoelig karakter. Dit betekent dat dit gewone en niet-bijzondere persoonsgegevens (zie pararagraaf 3.1.2) volgens de AVG zijn, en toch hebben deze persoonsgegevens een gevoelig karakter. Daardoor moeten wij met deze persoonsgegevens integer en vertrouwelijk omgaan.

Voorbeelden van gevoelige persoonsgegevens zijn:
- burgerservicenummer (bsn)
- strafrechtelijke gegevens
- financiële gegevens
- verklaring omtrent gedrag (vog)
- elektronische identificatiegegevens (locatiegegevens)
- verslagen van beoordelings- en/of functioneringsgesprekken
- gegevens over de persoonlijke situatie van een medewerker

Aan verwerken van het bsn en strafrechtelijke gegevens worden strenge eisen gesteld, waarbij de mogelijke verwerking is vastgelegd in specifieke wetgeving.

3.1.2 Bijzondere persoonsgegevens
De verwerking van bijzondere persoonsgegevens is verboden, tenzij wij het verwerkingsverbod op grond van de AVG kunnen opheffen. Als het verwerkingsverbod is opgeheven, moet de verwerking van bijzondere persoonsgegevens ook voldoen aan alle andere eisen van de AVG en dit privacybeleid. Zo moet de verwerking voldoen aan de beleidsbeginselen van paragraaf 2.2 van dit privacybeleid en moet de verwerking van bijzondere persoonsgegevens een doeleinde (paragraaf 3.2) en een grondslag (paragraaf 3.3) hebben.

We verwerken bij onze werkzaamheden bijzondere categorieën persoonsgegevens. Daarbij worden vooral de volgende gegevens verwerkt:
- gegevens over gezondheid
- gegevens die iets zeggen over ras of etnische afkomst
- gegevens met betrekking tot iemands seksueel gedrag
- gegevens over seksueel gedrag of seksuele gerichtheid

Zwaardere zorgvuldigheidseisen
Voor het verwerken van bijzondere persoonsgegevens gelden zwaardere zorgvuldigheidseisen, waaronder die voor de beveiliging. Daar waar de basisbescherming niet voldoende is, moeten wij voor elk informatiesysteem apart afgestemde extra maatregelen nemen om deze bijzondere persoonsgegevens te beschermen.

Wij betrekken bij het verwerken van bijzondere persoonsgegevens altijd de Privacy Officer en/of de Functionaris Gegevensbescherming.

3.1.3 BIV-classificatie SamenTwente
Wij hanteren een classificatiedocument ('BIV Classificatie SamenTwente') dat van toepassing is op alle documenten, informatie en informatiesystemen die onder de verantwoordelijkheid van SamenTwente vallen. Dit betekent dat gewone en gevoelige persoonsgegevens (onder a) en bijzondere persoonsgegevens (onder b) hier ook onder vallen.

3.2 Doeleinden verwerkingen persoonsgegevens

We omschrijven vooraf de doeleinden van de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking toetsen wij in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij wegen wij de verschillende belangen af en kijken wij naar de doelmatigheid, proportionaliteit en subsidiariteit. Wij verwerken persoonsgegevens overeenkomstig de beleidsprincipes altijd op een manier die verenigbaar is met de doeleinden waarvoor we ze hebben gekregen.

De doeleinden waarvoor wij persoonsgegevens verwerken zijn onder andere:

1. Uitvoeren van wettelijke taken, onder andere:
   - GGD-taken
   - VTT-taken
   - OZJT-taken
2. Personeelszaken, onder andere:
   - Werving & selectie nieuwe medewerkers
   - Personeelsadministratie, waaronder beoordelingen en verzuim
   - Salarisadministratie
3. Bedrijfsvoering en financiën, onder andere:
   - Financiële administratie
   - Beheren van het inkoopsystemen en betaalsystemen
4. ICT-zaken, onder andere:
   - Beheren van ICT-middelen
   - Authenticatiemogelijkheden
   - Digitale toegang
5. Facilitaire en algemene zaken, onder andere:
   - Fysieke toegang
   - Reservering vergaderzalen
   - Klachtenprocedure

Wij gebruiken Security Operation Centers (SOC). Een SOC monitort en onderzoekt afwijkende gedragingen van medewerkers in systemen. SamenTwente zorgt ervoor dat wij met de werkzaamheden van het SOC voldoen aan de AVG.

3.3 Grondslag verwerking

Wij zorgen altijd voor een rechtsgeldige grondslag voor de verwerking en leggen deze vast in het register van verwerkingen. De AVG kent de volgende grondslagen volgens artikel 6:

- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting
- De verwerking is noodzakelijk voor de vervulling van een tak van algemeen belang of uitoefening van openbaar gezag
- De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoons te verwerken
- De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang.

Het verwerken van bijzondere persoonsgegevens, zoals gezondheidsgegevens, is in beginsel verboden. Artikel 9 lid 2 AVG biedt de uitzonderingsgronden om toch bijzondere persoonsgegevens te mogen verwerken. Ook is het ons niet toegestaan om voor de publiekrechtelijke en wettelijke taken persoonsgegevens te verwerken op basis van de grondslag gerechtvaardigd belang.

Afweging belangen
Als wij op basis van gerechtvaardigd belang persoonsgegevens verwerken, dan zorgt het management dat er een afweging plaatsvindt tussen de belangen van betrokkenen (zijn grondrechten en de fundamentele vrijheden) en de belangen van SamenTwente. Het management legt de uitkomsten hiervan ter toetsing voor aan de Functionaris Gegevensbescherming.

Expliciete toestemming
Als wij op basis van toestemming persoonsgegevens verwerken, dan is de toestemming altijd een expliciete toestemming, die wij in duidelijke en leesbare taal hebben opgesteld. Het management zorgt dat het kan aantonen dat betrokkene toestemming heeft gegeven. Ook zorgen wij ervoor dat betrokkene de toestemming op een eenvoudige manier kan intrekken. Voor kinderen gelden extra eisen voor het vragen van toestemming.

3.4 Bewaartermijn persoonsgegevens
Wij bewaren persoonsgegevens niet langer dan redelijkerwijs noodzakelijk is. Wij voeren een bewaartermijnenbeleid waarin wij zoveel mogelijk de wettelijke bewaartermijnen hanteren aangevuld met de VNG Selectielijst. Dit beleid staat beschreven in een apart beleidsdocument: *Bewaartermijnenbeleid SamenTwente*.

Vernietiging persoonsgegevens
Wij moeten persoonsgegevens na het verlopen van de bewaartermijn buiten het bereik van de actieve administratie brengen. De persoonsgegevens vernietigen we na het verlopen van de bewaartermijn. Of, als dit niet mogelijk is, anonimiseren we deze gegevens. Bij iedere verwerking bepalen wij vooraf wat de bewaartermijnen zijn of de criteria voor de gebruikstermijn voor verwijdering.

3.5 Werkprocessen
Wij zorgen voor werkprocessen, zodat medewerkers weten wat wij van hen verwachten voor de werkzaamheden die zij uitvoeren. In deze werkprocessen staat beschreven hoe zij de persoonsgegevens moeten verwerken. Bij iedere verwerking stellen wij de werkprocessen op voor de verwerking is gestart. Als blijkt dat werkprocessen niet zijn opgesteld of onvolledig zijn, stelt de verantwoordelijke manager/ proceseigenaar deze werkprocessen zo snel en zo volledig mogelijk op.

3.6 Gegevensuitwisseling (doorgifte)
In bepaalde gevallen kan het voorkomen dat wij persoonsgegevens delen met andere partijen. Uitgangspunt is dat wij alleen persoonsgegevens delen als dat noodzakelijk is voor de procedure of als wij hiertoe wettelijk verplicht zijn. Per geval beoordelen wij of het delen van persoonsgegevens noodzakelijk is. Wij zijn verantwoordelijk voor het eindoordeel en het maken van de juiste afspraken hierover. Als wij niet de verwerkingsverantwoordelijke zijn van de persoonsgegevens, stemmen we de uitwisseling eerst af met de verwerkingsverantwoordelijke(n).

3.6.1 Verwerking uitbesteden aan een (sub)verwerker
Wij laten namens ons en op grond van onze instructies persoonsgegevens door een (sub)verwerker verwerken. We schakelen alleen verwerkers in die afdoende garanties bieden voor het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. Om deze persoonsgegevens te beschermen tegen de verschillende risico's, treffen we passende beveiligingsmaatregelen overeenkomstig het beveiligingsbeleid van SamenTwente.

Verwerkingsovereenkomst

- De afspraken over de verwerking door de verwerker leggen we schriftelijk vast in een verwerkingsovereenkomst. Deze toetsen we voordat de dienstverlening aanvangt en daarna ten minste eenmaal per drie jaren.
- Een systeem mag pas in gebruik worden genomen als de verplichte verwerkingsovereenkomst is ondertekend. Wij controleren steekproefsgewijs en ten minste eenmaal per drie jaren of de verwerkers voldoen aan de afspraken uit de verwerkersovereenkomst. De verwerkingsovereenkomst vormt een aanvulling op de hoofdovereenkomst.
- De Functionaris Gegevensbescherming stelt het model vast waar de standaardverwerkingsovereenkomst minimaal aan moet voldoen. De verantwoordelijke voor de verwerking, zoals de projectleider, zorgt dat wij een verwerkingsovereenkomst aangaan en naleven daar waar sprake is van een verwerker. Onze Privacy Officer biedt hierbij ondersteuning.
- Wij ondertekenen de verwerkingsovereenkomst en we zorgen dat de Privacy Officer deze ontvangt. De Privacy Officer houdt ook een overzicht bij van alle aangeleverde verwerkingsovereenkomsten. Dit doet de Privacy Officer enkel voor overzicht en toezicht, niet als feitelijke beheerder.

3.6.2 Andere afspraken – samenwerkingspartijen en gezamenlijke verantwoordelijke

Verder kan het voorkomen dat we een andere partij inschakelen of met andere partijen samenwerken, die geen verwerker zijn, maar waarmee we wel persoonsgegevens uitwisselen. Ook dan maken wij passende afspraken. In dat geval zullen wij een overeenkomst sluiten over de verwerking van persoonsgegevens, of samen met de andere partij een regeling vaststellen, waarin wij de verantwoordelijkheden vastleggen.

Rollen en verantwoordelijkheden

- Als we een samenwerkingsverband aangaan, hebben de partijen vaak een gezamenlijk doel dat zij bepalen en nastreven. Volgens artikel 26 van de AVG maken wij duidelijke afspraken over de rollen en verantwoordelijkheden die de samenwerkende partijen hebben. Daarnaast moet het voor de betrokkenen helder zijn waar en bij wie zij hun vragen kunnen stellen en waar zij zich op hun rechten kunnen beroepen. Wij maken zulke afspraken via een overeenkomst tussen gezamenlijk verantwoordelijken.
- De verantwoordelijke voor de verwerking, zoals de manager, zorgt en waakt ervoor dat wij een gezamenlijke verantwoordelijkenovereenkomst aangaan daar waar een gezamenlijke verwerkingsverantwoordelijkheid is. De Privacy Officer kan hierbij ondersteunen.

3.6.3 Verwerking binnen de Europese Economische Ruimte (EER)

We verstrekken over het algemeen persoonsgegevens aan organisaties die zich binnen de EER bevinden. Denk hierbij aan een verwerker en ook aan samenwerkingspartners. De EER bestaat uit alle lidstaten van de Europese Unie en drie EVA-lidstaten, namelijk Noorwegen, IJsland en Liechtenstein. De AVG is rechtstreeks van toepassing binnen alle lidstaten van de Europese Unie en tevens binnen de EER.

De verantwoordelijke voor de verwerking, zoals de manager, zorgt dat we bij gegevensuitwisseling binnen de EER voldoen aan de eisen van de AVG.

3.6.4 Verwerking buiten de EER

We verstrekken in beginsel geen persoonsgegevens aan organisaties (een (sub)verwerker of samenwerkingspartner) die zich buiten de EER bevinden. Als dit wel gebeurt, zorgen we dat we altijd rekening houden met de eisen van de AVG.

De AVG is niet rechtstreeks van toepassing voor organisaties buiten de EER. Om die reden zijn we verplicht een extra controle te hanteren tot het beschermingsniveau van het desbetreffende land.

- We hanteren als eerste uitgangspunt de lijst met landen met een passend beschermingsniveau van de Europese Commissie, de zogenoemde adequaatheidsbesluiten. Landen buiten de EER waarvoor een adequaatheidsbesluit geldt, moeten op grond van eigen wet- en regelgeving een passend beschermingsniveau bieden. Daardoor hoeven we geen aanvullende maatregelen te nemen om de persoonsgegevens te beschermen.
- Landen waarvoor geen adequaatheidsbesluit geldt, bieden niet op grond van eigen wet- en regelgeving een passend beschermingsniveau voor de verwerking van persoonsgegevens. Wij verstrekken in dat geval alleen persoonsgegevens als wij er andere passende waarborgen volgens de AVG zijn. Een voorbeeld is het afsluiten van de standaard modelcontracten voor veilige doorgifte van persoonsgegevens.

Rollen en verantwoordelijkheden

- De verantwoordelijke voor de verwerking, zoals de manager, zorgt dat wij daar waar nodig passende waarborgen nemen om de persoonsgegevens van betrokkene bij gegevensuitwisseling buiten de EER te beschermen. De Privacy Officer kan hierbij ondersteuning bieden.
- Als het treffen van passende waarborgen niet mogelijk is, geven wij alleen persoonsgegevens door aan landen buiten de EER of internationale organisaties conform artikel 49 AVG. Een voorbeeld is de uitdrukkelijke toestemming van de betrokkene voor de gegevensuitwisseling buiten de EER.
- Het kan zijn dat de Functionaris Gegevensbescherming adviseert aanvullende maatregelen te treffen, zoals het uitvoeren van een data transfer impact assessment.

3.7 Geheimhouding extern en intern

Alle persoonsgegevens behandelen we als vertrouwelijk. Dit betekent onder andere dat persoonsgegevens niet mogen worden gedeeld, gepubliceerd, ingezien of anderszins mogen worden verwerkt, zonder dat daarvoor een geldige noodzaak is. Iedereen hoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennisnemen. Ze zijn hier alleen niet toe verplicht als enig wettelijk voorschrift hen tot mededeling verplicht of als uit hun taak de noodzaak tot mededeling voortvloeit.

Waarborgen geheimhouding

- Wij waarborgen deze geheimhouding voor interne medewerkers via de arbeidsovereenkomst en/of de daarbij geldende collectieve arbeidsovereenkomst en doordat zij bij indiensttreding de eed of de belofte afleggen.
- Externe medewerkers ondertekenen voor de geheimhoudingsplicht een overeenkomstige geheimhoudingsverklaring.
- Wij binden verwerkers, hun medewerkers en door hen ingeschakelde partijen aan geheimhouding via de verwerkingsovereenkomst.

4 Governance en organisatorische borging gegevensverwerking

Het goed, efficiënt en verantwoord leiden van een organisatie duiden we vaak aan met de term governance. Het omvat vooral ook de relatie met onze belangrijkste belanghebbenden. Een goede governance borgt privacy binnen SamenTwente en waarborgt de rechten van alle betrokkenen. Hoe wij governance inrichten binnen onze organisatie, beschrijven we in dit hoofdstuk.

4.1 Rollen en verantwoordelijkheden privacy

Ons doel is om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd uit te voeren. Daarvoor beschrijven we allereerst een aantal rollen en verantwoordelijkheden.

4.1.1 Dagelijks bestuur

Het dagelijks bestuur is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen SamenTwente. Het dagelijks bestuur:

- stelt het beleid vast en draagt ervoor zorg dat wij aan de wettelijke eisen uit de AVG voldoen;
- stelt een Functionaris Gegevensbescherming aan die voldoende middelen heeft om zijn of haar taak uit te oefenen;
- stelt voldoende middelen beschikbaar om de gegevensbeschermingen binnen SamenTwente te laten voldoen aan de gestelde eigen vereisten en wettelijke verplichtingen;
- stelt voldoende middelen beschikbaar om informatiebewustzijn binnen de organisatie te borgen.

4.1.2 Directeur en Centraal Management Team

De Directeur en het Centraal Management Team zijn verantwoordelijk: zij zorgen dat de werkprocessen voldoen aan de wet- en regelgeving voor het beschermen van de persoonsgegevens. De Directeur en het Centraal Management Team:

- stellen de procedures en maatregelen vast voor het beschermen van de persoonsgegevens binnen de kaders van het privacybeleid;
- stimuleren bewustwording en naleving van het beleid als onderdeel van de integrale bedrijfsvoering.

4.1.3 Management

Het management van de afdelingen en teams is intern verantwoordelijk voor het voldoen aan de wet- en regelgeving rondom de bescherming van persoonsgegevens binnen de eigen afdeling. Onderdeel van de integrale bedrijfsvoering is het creëren van bewustwording en de naleving van het beleid. Het management heeft daarin de taak om:

- te zorgen dat haar medewerkers op de hoogte zijn van (de voor hun relevante aspecten van) het beleid;
- de medewerkers te faciliteren bij de naleving van dit beleid en tijd te geven om trainingen te volgen en om aan bewustwordingsactiviteiten deel te nemen;
- aantoonbaar toe te zien op de naleving van het beleid door haar medewerkers;
- periodiek het onderwerp bescherming van persoonsgegevens onder de aandacht te brengen in werkoverleggen;
- de proceseigenaar, de systeembeheerder en contractbeheerder te informeren over hun verantwoordelijkheden voor de bij hun proces, systeem en/of contract horende taken en privacy processen.

Jaarlijks leggen de managers verantwoording af aan het CMT over de nakoming van de regels voor de bescherming van Persoonsgegevens. Het management kan zich hierin laten ondersteunen door de Functionaris Gegevensbescherming en/of de Privacy Officer.

4.1.4 Proceseigenaar

De proceseigenaar is ervoor verantwoordelijk dat het contract, de verwerking en/of de applicatie en bijbehorende ICT-faciliteiten (informatiesysteem) en/of het werkproces voldoen aan het beleid. Dit betekent dat de proceseigenaar zorgt dat het informatiesysteem en werkproces blijven voldoen aan de eisen en wensen van de gebruikers en ook aan de wet- en regelgeving, zoals de bescherming van persoonsgegevens. De proceseigenaar:

- toetst met een pre-DPIA of het uitvoeren van een DPIA verplicht is. Als dit verplicht is, zal de eigenaar zorgen voor het uitvoeren van een DPIA en periodiek/situationeel toetsen of de DPIA nog actueel is. De Privacy Officer kan de proceseigenaar hierin ondersteunen;
- zorgt dat er verwerkingsovereenkomsten met leveranciers afgesloten zijn en dat ze actueel blijven;
- zorgt dat bewaartermijnen goed ingericht zijn in systemen en processen;
- zorgt dat het register van verwerkingen gevuld is en actueel blijft;
- zorgt dat systemen passend beveiligd zijn en blijven en voldoen aan de eisen van privacy doordat ontwerp en privacy vriendelijke instellingen doorgevoerd zijn.

4.1.5 Medewerkers

Al onze medewerkers zijn verantwoordelijk voor een rechtmatige omgang met persoonsgegevens. Wij verwachten van medewerkers dat zij zich integer gedragen en geen gedrag vertonen en situaties laten ontstaan die kunnen leiden tot inbreuken op de rechten en vrijheden van de betrokkenen en schade voor SamenTwente. Daarvoor hebben wij de beleidsprincipes in paragraaf 2.2 opgesteld. Deze beleidsprincipes vormen ook het kader als wij onze procedures en de werkprocessen vaststellen of aanpassen.

4.1.6 Functionaris Gegevensbescherming (FG)

De FG houdt binnen SamenTwente toezicht op de toepassing en naleving van de wet- en regelgeving rondom privacy en het privacybeleid. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG ontvangt geen instructies over het uitvoeren van de toezichthoudende taak. De FG kan niet ontslagen worden of een sanctie krijgen als gevolg van de uitoefening van diens taken.

De FG heeft als interne toezichthouder toegang tot alle (interne) stukken en locaties, materialen en ondersteuning die nodig zijn om adequaat toezicht te kunnen houden. Directeur, management en medewerkers verstrekken de FG daarbij desgevraagd alle inlichtingen en medewerking. Als de FG dit naar redelijkheid nodig vindt, kan de FG voor diens onderzoek gebruikmaken van de diensten van externe specialisten. Wij stellen de FG voldoende middelen ter beschikking om diens taken naar behoren te kunnen uitvoeren.

Wij betrekken de FG vroegtijdig bij ontwikkelingen over alle zaken die verband houden met de bescherming van persoonsgegevens. Hierbij is het belangrijk dat:

- wij de FG regelmatig uitnodigen om vergaderingen van het hogere management en het middenkader bij te wonen en ten minste wanneer wij beslissingen nemen die gevolgen hebben voor de gegevensbescherming;
- de FG vooraf alle relevante informatie ontvangt over voorgenomen aanpassingen in de gegevensbescherming, zodat de FG een passend advies kan geven;
- wij de mening van de FG als zwaarwegend in overweging nemen waarbij wij, in geval van onenigheid, onderbouwd documenteren waarom wij het advies van de FG niet volgen;
- wij de FG meteen consulteren zodra zich een gegevensinbreuk of ander incident voordoet.

De taken van de Functionaris Gegevensbescherming zijn ten minste:

- adviseert gevraagd en ongevraagd de directeur en het CMT op strategisch niveau en over alle aspecten van bescherming persoonsgegevens;
- adviseert en informeert de organisatie en de afzonderlijke organisatieonderdelen over het toepassen van de privacy wet- en regelgeving en bevordert het bewustzijn van medewerkers over de bescherming van persoonsgegevens;
- adviseert zwaarwegend over het privacybeleid, reglementen en richtlijnen en aanpassingen daarvan. De FG stelt de modellen vast waaraan de privacyverklaring, het verwerkingsregister, de verwerkingsovereenkomst, de DPIA, pre-DPIA, de privacy-procedures en andere privacy-stukken minimaal moeten voldoen;
- adviseert zwaarwegend over de uitgevoerde pre-DPIA's en DPIA's. Wij betrekken de FG vanaf een vroegtijdig stadium bij het DPIA-proces, vooral in geval van een nieuwe verwerking. Als wij het advies van de FG niet volgen, dan documenteren wij deze beslissing onderbouwd;
- adviseert zwaarwegend over de afhandeling van privacy-klachten en -bezwaarschriften en over de procedure voor de behandeling van AVG-verzoeken. De FG is aanspreekpunt en vraagbaak voor degenen die vragen hebben over de bescherming van persoonsgegevens;
- houdt intern toezicht op de naleving van de AVG, overige privacy wet- en regelgeving en het privacybeleid. De FG informeert en adviseert de directeur en het verantwoordelijke management als blijkt dat wij het privacybeleid niet op een juiste wijze uitvoeren;
- rapporteert ten minste eenmaal per jaar aan het dagelijks bestuur en de directeur over diens bevindingen, waaronder de geregistreerde datalekken en de naleving van de geadviseerde verbeteringen;
- adviseert gevraagd en ongevraagd bij constateringen van misstanden en ondermaatse technische en organisatorische beveiligingsmaatregelen. Zo nodig treft de FG aanvullende acties, zoals het escaleren bij het dagelijks bestuur en/of het inwinnen van advies bij de Autoriteit Persoonsgegevens;
- treedt op als contactpersoon van SamenTwente voor de Autoriteit Persoonsgegevens (AP), meldt datalekken bij de AP en werkt met de AP samen. Als de AP een onderzoek instelt binnen SamenTwente kan de FG niet namens SamenTwente spreken. Wel houden wij de FG op de hoogte van de communicatie tussen de AP en SamenTwente.

De FG houdt bij de uitvoering van diens taken rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

4.1.7 Privacy Officer (PO)

De Privacy Officer is het eerste interne aanspreekpunt voor alle privacy gerelateerde vragen, klachten en datalekken binnen SamenTwente. De Privacy Officer heeft daarnaast een rol (ondersteunend aan de proceseigenaren) in:

- het invullen en actueel houden van het verwerkingenregister;
- het beoordelen van (concept)verwerkingsovereenkomsten;
- het uitvoeren van DPIA's en pre-DPIA's (dit is een check of een DPIA verplicht is).

Andere taken van de Privacy Officer zijn ten minste:

- is het eerste interne aanspreekpunt voor privacy-gerelateerde vragen;
- ondersteunt de afdelingen bij het uitvoeren van de rechten van betrokkenen;
- wikkelt datalekken af in afstemming met de FG;
- voert DPIA's en pre-DPIA's uit met ondersteuning van informatiemanagers en medewerkers die inhoudelijk in het proces werken en in afstemming met de FG;
- ondersteunt de informatiemanagers, managers en projectleiders bij awareness(campagnes)
- ondersteunt bij het opstellen van privacy-procedures;

- stelt in afstemming met de FG triaalrapportages op over de bescherming van persoonsgegevens, waaronder de geregistreerde datalekken (paragraaf 4.3);
- ondersteunt de Functionaris Gegevensbescherming in de uitvoering van diens taken.

4.2 Rollen en verantwoordelijkheden informatiebeveiliging (IB)

Informatiebeveiliging en gegevensbescherming zijn verwante verantwoordelijkheidsgebieden. Deze raken en vinden elkaar in de beveiliging van persoonsgegevens.
Privacy ziet vooral toe op rechtmatigheid, behoorlijkheid en transparantie (zie de beleidsuitgangspunten in paragraaf 2.2). Informatiebeveiliging ziet vooral toe op de betrouwbaarheid van de informatie met als belangrijkste criteria: beschikbaarheid, integriteit en vertrouwelijkheid (BIV) (zie paragraaf 5.3).

Binnen informatiebeveiliging worden de volgende rollen en verantwoordelijkheden onderscheiden:

- Chief Information Security Officer (CISO)
- Information Security Officer (ISO)

Het IB-beleid inclusief deze rollen en verantwoordelijkheden staan beschreven in een apart beleidsdocument: *Informatiebeveiligingsbeleid SamenTwente.*

4.3 Planning & Control-cyclus

SamenTwente hanteert een Planning & Control-cyclus (P&C-cyclus). We leggen bestuurlijk verantwoording af in de jaarrekening met het jaarverslag en in bestuursrapportages. De interne controlecyclus vindt driemaal per jaar plaats.

De Functionaris Gegevensbescherming stelt jaarlijks een FG-rapportage op over de bescherming van persoonsgegevens en stuurt deze naar het dagelijks bestuur en de directeur. Daarnaast stelt de FG in afstemming met de Privacy Officer elke vier maanden een rapportage over de bescherming van persoonsgegevens op. Daarin staan ten minste:

- de voortgang van de actuele zaken;
- nieuwe vraagstukken;
- de aanvullingen van het verwerkingenregister;
- het aantal beoordeelde en goedgekeurde verwerkersovereenkomsten;
- het aantal en de aard van incidenten/klachten, datalekken (gemeld en ongemeld bij de AP);
- de uitgevoerde DPIA's en/of audits met een samenvatting van de resultaten.

5 Risicobeheersing

Een belangrijk onderdeel van gegevensverwerking en de bescherming van de rechten van betrokkenen is het beheersen van risico's. Risicobeheersing is een constant proces dat wij in acht moeten nemen vanaf het moment dat wij persoonsgegevens verzamelen tot aan het moment dat wij deze verwijderen. Om alle mogelijke risico's van gegevensverwerking in kaart te brengen en deze te kunnen beheersen, zijn Privacy by Design, Privacy by Default, DPIA's, passende beveiligingsmaatregelen, awareness en het afleggen van verantwoording noodzakelijk. We beschrijven deze principes in dit hoofdstuk.

5.1 Privacy by Design en Privacy by Default

Als wij procedures en werkprocessen inrichten of als wij producten en diensten aanschaffen, ontwerpen en inrichten hanteren wij de principes van 'Privacy by Design' en 'Privacy by Default'. Hiermee borgen wij privacyaspecten en de bescherming van persoonsgegevens vanaf het begin. Daardoor beperken of voorkomen wij risico's voor de rechten en vrijheden van de betrokkene aan de voorkant.

5.1.1 Privacy by Design (gegevensbescherming door ontwerp)

Als wij een product of dienst ontwerpen of als wij procedures en werkprocessen inrichten, houden wij vanaf het begin rekening met de uitgangspunten van de AVG en de daarbij horende technische en organisatorische maatregelen. De aandacht hiervoor blijft tijdens de hele levenscyclus van de gegevens bij SamenTwente bestaan. Op deze manier houden wij rekening met:

- welke persoonsgegevens daadwerkelijk noodzakelijk zijn voor het doel waarvoor wij ze verzamelen;
- of wij deze persoonsgegevens kunnen beveiligen;
- hoelang we de persoonsgegevens mogen bewaren;
- wie toegang heeft tot het systeem en welke rechten daaraan zijn verbonden, zoals: wie mag welke gegevens inzien, kopiëren, verwerken, wijzigen en verwijderen.

Wij onderwerpen elke nieuwe verwerking aan een checklist om ervoor te zorgen dat wij de privacy van betrokkenen waarborgen. Deze checklist raadplegen we voor wij een verwerking starten en we volgen de lijst compleet tijdens het opzetten van de verwerking. Hieronder staan voorbeelden.

Minimaal gebruik van persoonsgegevens

- Wij verzamelen (of vragen om) niet meer gegevens dan noodzakelijk.
- Wij verwerken alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerken deze verder alleen op een manier die verenigbaar is met dit doel.
- Bij configuratie van systemen kiezen wij altijd voor de privacy-vriendelijke variant en privacy-vriendelijke instellingen.
- De informatie die wij verwerken is correct en actueel.
- Wij maken geen onnodige kopieën.
- Wij verwijderen wat niet meer nodig is.

Passende bescherming

- Wij slaan gegevens zo op dat wij kunnen voldoen aan de wettelijke kaders van de AVG. Dit betekent in verband met de doelbinding vaak gescheiden opslag.
- Wij beperken de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben.
- Wij beschermen persoonsgegevens door deze gegevens o.a. te aggregeren, versleutelen en anonimiseren. Hierdoor verminderen wij de mate waarin de verwerkte persoonsgegevens kunnen worden herleid.

Als uitgangspunt kiezen wij voor technische maatregelen om de privacy door ontwerp te waarborgen. Als de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen, zoeken wij naar organisatorische en/of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit werken wij uiteraard uit samen en in overleg met de CISO.

5.1.2 Privacy by Default (gegevensbescherming door standaardinstellingen)

Wij zorgen ervoor dat wij technische en organisatorische maatregelen nemen waarbij wij als standaard alleen die persoonsgegevens verwerken die ook daadwerkelijk noodzakelijk zijn voor het specifieke doel van de verwerking. Dit betekent dat wij bijvoorbeeld bij de instellingen van een programma, een applicatie, een website of een dienst maximale privacy uitvoeren (opt-in), zonder dat de betrokkene deze instelling zelf AVG-compliant moet instellen. Wij zorgen en waken ervoor dat wij deze principes naleven. De Privacy Officer en Functionaris Gegevensbescherming kunnen ondersteuning bieden waar nodig.

5.2 Data Protection Impact Assessment (DPIA)

Bij elke nieuwe verwerking moet SamenTwente de privacy-risico's en de getroffen maatregelen beoordelen, ongeacht of we dit in de vorm van een DPIA doen. Wij voeren standaard een DPIA uit bij nieuwe verwerkingen, zoals projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen die een mogelijk hoog risico voor de privacyrechten en -vrijheden van betrokkenen opleveren. SamenTwente werkt vaak met gevoelige of bijzondere gegevens. Een DPIA is dan al snel nodig.

Met de DPIA beoordelen wij onder meer de risico's van een voorgenomen verwerking en brengen wij deze op een gestandaardiseerde wijze in kaart. Op basis hiervan treffen wij maatregelen om de geconstateerde risico's te verlichten of te voorkomen. Wanneer een hoog risico blijft, moeten wij een voorafgaande raadpleging vragen bij de Autoriteit Persoonsgegevens.

Wij voeren de DPIA uit voorafgaand aan een nieuwe verwerking en achteraf bij bestaande verwerkingen als een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen.

DPIA-proces

Voor het DPIA-proces gelden deze kaders:

1. Wij houden een DPIA voordat wij starten met de betreffende verwerking.
2. Wij herhalen een DPIA periodiek op onderdelen ter evaluatie, en ook bij wijzigingen waardoor de risico's van de verwerking toenemen. Wij herhalen een DPIA eerder dan de vastgestelde termijn voor de betreffende verwerking(en), als het werkproces substantieel wijzigt en/of wij een nieuw informatiesysteem gebruiken.
3. Bij het uitvoeren van een DPIA betrekken wij de FG altijd op tijd.
4. Het verantwoordelijke management ziet toe op het nemen van maatregelen die volgens de DPIA nodig zijn om de risico's te verkleinen of geheel weg te nemen.
5. Wij leggen het resultaat van de DPIA en de genomen maatregelen om het risico te beperken ter beoordeling voor aan de FG (FG-advies).
6. Als het verantwoordelijke management niet in staat is om voldoende maatregelen te treffen om de risico's te beperken, vragen wij de AP om een voorafgaande raadpleging.
7. DPIA's die wij binnen SamenTwente uitvoeren vinden plaats volgens de SamenTwente-standaard en overeenkomstig het proces.

Als blijkt dat wij een DPIA moeten uitvoeren, dan maakt het management hier capaciteit voor vrij en ondersteunt de proceseigenaren in het uitvoeren van de DPIA. De proceseigenaar voert een DPIA uit in overeenstemming met het DPIA-proces. De Privacy Officer ondersteunt hierin. De proceseigenaar waakt ervoor dat de DPIA tijdig wordt uitgevoerd. De Privacy Officer beschikt over de pre-DPIA vragenlijst en een DPIA-register met alle uitgevoerde DPIA's, zodat wij op deze wijze kunnen voldoen aan onze verantwoordingsplicht.

De verantwoordelijke manager betrekt de Functionaris Gegevensbescherming tijdig bij het DPIA-proces. De Functionaris Gegevensbescherming voorziet de definitieve DPIA daarnaast van een formeel advies.

5.2.1 Privacyrisico's

Wij toetsen aan de hand van de pre-DPIA, een vragenlijst, of er een hoog privacyrisico is en daarmee de noodzaak tot het uitvoeren van een (uitgebreide) DPIA. Op grond van de AVG is er in ieder geval een hoog privacyrisico als wij:

- systematisch en uitvoerig persoonlijke aspecten evalueren, zoals profiling; of
- op grote schaal bijzondere persoonsgegevens verwerken of op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied. Hierbij letten wij op het aantal betrokkenen, het volume van gegevens en/ of het bereik van verschillende gegevens/ items die wij verwerken, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit; of
- voldoen aan één of meer van de 17 situaties op de lijst van Autoriteit Persoonsgegevens; of
- voldoen aan twee of meer van de negen criteria op de lijst van de voormalige werkgroep van Europese privacy-toezichthouders (WP29, nu genoemd EDPB).

Wij brengen de risico's in kaart aan de hand van de MAPGOOD-methode. MAPGOOD staat voor Mensen, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten. Dit zijn verschillende invalshoeken om naar bedreigingen en risico's te kijken.

Passende beveiligingsmaatregelen

Burgers, medewerkers en andere betrokkenen vertrouwen (gevoelige) persoonsgegevens toe aan SamenTwente. Wij verwerken deze gegevens in onze organisatie en informatiesystemen in het kader van de uitvoering van onze taak en werkzaamheden. Wij zijn verantwoordelijk voor het inrichten, onderhouden en continu verbeteren van passende beveiliging van deze persoonsgegevens. Wij zorgen daarom voor een passend beveiligingsniveau en wij voeren passende technische en organisatorische maatregelen uit. Deze maatregelen zijn in lijn met de wettelijke verplichting, onze eigen organisatierisico's en het vertrouwen en belangen van de betrokkenen.

5.2.2 Informatiebeveiliging

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een van de randvoorwaarden voor het borgen van privacy bij de verwerking van persoonsgegevens. Met de beveiligingsmaatregelen willen wij persoonsgegevens beschermen tegen verlies en tegen onrechtmatige verwerking. Ook willen wij hiermee materiële en/of immateriële schade van betrokkenen en de organisatie beperken en/of voorkomen.

Waar passend omvatten de beveiligingsmaatregelen volgens artikel 32 AVG onder meer het volgende. Wij:

a. pseudonimiseren en versleutelen persoonsgegevens;
b. kunnen op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten garanderen;
c. kunnen bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens herstellen;
d. hebben een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking;
e. sluiten verwerkingsovereenkomsten af met verwerkers.

Wij leggen de te nemen beveiligingsmaatregelen ter toetsing voor aan de CISO en de FG. In het document *Informatiebeveiligingsbeleid SamenTwente* vind je de beveiligingsmaatregelen en het kader rondom beveiliging van informatie en persoonsgegevens.

Informatiebeveiligingsbeleid
Wij hanteren een informatiebeveiligingsbeleid voor het gehele proces van informatievoorziening, inclusief de niet geautomatiseerde stappen waarin nog papieren gegevens of dossiers worden uitgewisseld. De CISO ziet toe op de naleving van het informatiebeveiligingsbeleid binnen SamenTwente.

Informatiebeveiliging is de verzamelnaam voor de maatregelen die wij nemen om de betrouwbaarheid van informatie te waarborgen. Wij duiden de vereiste mate betrouwbaarheid van de (persoons)gegevens en andere informatie ook wel aan als 'BIV':

- *Beschikbaarheid*: zorgen dat de informatie en informatiesystemen beschikbaar en toegankelijk zijn voor de gebruikers
- *Integriteit*: waarborgen dat de informatie en informatieverwerking correct zijn, volledig, actueel en controleerbaar
- *Vertrouwelijkheid*: beschermen van de informatie tegen kennisname, mutatie, toevoeging of vernietiging door onbevoegden. Zorgen dat de informatie alleen toegankelijk is voor personen die daar vanuit hun rol/ functie toegang toe mogen hebben.

Wij streven deze doelen van betrouwbare informatie en een veilig en zorgvuldig gebruik van informatie en informatiesystemen na. Wij sluiten daarvoor aan bij de ontwikkelde kaders en maatregelen in standaard (informatie)beveiligingsnormen.

5.2.3 Normen voor Informatiebeveiliging (IB) en Privacy-informatiemanagement (PIM)

De basis informatiebeveiligingsnormen (IB-normen) zijn NEN-ISO/IEC 27001:2022 en NEN-ISO/IEC 27002:2022. Voor SamenTwente gelden de hiervan afgeleide normen:

- BIO (Baseline Informatiebeveiliging Overheid), ontwikkeld voor overheden en
- NEN 7510, 7512 en 7513 ontwikkeld voor medische informatiesystemen zoals SamenTwente deze als zorgaanbieder gebruikt.

Daarnaast zijn onder meer de normen ISO 27017:2021 voor clouddiensten en ISO 27701:2021 voor privacy-informatiemanagement van belang.

We verwachten dat in 2025 de BIO versie 2.0 wettelijk verplicht wordt voor overheden. De maatregelen zijn daarin ingedeeld in vier thema's: mens, fysiek, technologie en organisatie. De verplichting wordt waarschijnlijk vastgelegd in de Cyberbeveiligingswet, waarin de Europese NIS2-richtlijn (beveiliging Netwerk- en Informatiesystemen) wordt geïmplementeerd.

Als zorgaanbieder zijn we wettelijk verplicht de NEN 7510, 7512 en 7513 als normenkader toe te passen voor een veilig en zorgvuldig gebruik van hun medische informatiesystemen. Dit volgt uit artikel 15j van de 'Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg' en de artikelen 3 en 5 van het 'Besluit elektronische gegevensverwerking door zorgaanbieders'. Daarbij is:

- NEN 7510 een managementsysteemnorm
- NEN 7512 een aanvulling voor gegevensuitwisseling tussen zorgaanbieders en
- NEN 7513 een aanvulling voor logging van het gebruik van de elektronische patiëntendossiers (EPD's)

Privacy-informatiemanagementsysteem (PIMS)
Wij streven ernaar ook te voldoen aan de privacy-informatiemanagementnorm 27701. Deze norm geeft maatregelen in aanvulling op de ISO 27001 en 27002 om het ISMS beter aan te laten sluiten op de eisen van AVG (PIMS). De ISO 27701 gebruikt het begrip PII (persoonlijk identificeerbare informatie). Dit komt uit Amerika en wijkt iets af van het AVG-begrip persoonsgegeven, waar ook pseudonieme gegevens onder vallen.

5.3 Awareness (bewustwording en training)

Awareness is een belangrijke stap voor AVG-compliance. Een privacybeleid en maatregelen om gegevensbescherming te waarborgen zijn niet voldoende om risico's uit te sluiten. Het is noodzakelijk om bij medewerkers (zowel intern als extern) voortdurend en actief het bewustzijn over privacy, informatiebeveiliging en gegevensbescherming aan te scherpen. Hiermee kunnen wij gedragsverandering realiseren, veilig en verantwoord gedrag aanmoedigen en verhogen wij kennis van gegevensbescherming en de daarmee gepaard gaande risico's.

5.3.1 Bewustwordingscampagnes

Wij willen om die reden de onderwerpen privacy, gegevensbescherming en informatiebeveiliging in de organisatie levend houden. Terugkerende bewustwordingscampagnes vormen hier een belangrijk onderdeel van. Deze campagnes kunnen aansluiten op andere beveiligingscampagnes.

Wij zullen awareness vergroten door:

- voorlichtende communicatie rond privacy- en securitythema's in allerlei vormen (presentaties, workshops, blogs en artikelen, flyer en poster campagne);
- een Q&A over privacy, gegevensbescherming en informatiebeveiliging op kennisnet te plaatsen;
- cursussen en trainingen te organiseren (kennisniveau verhogen);
- mystery guest bezoek te faciliteren (opzoeken van kwetsbaarheden tijdens bezoek en rapportage opleveren hierover die aan de medewerkers wordt teruggekoppeld) en toepassen van social engineering;
- gedragsregels op te stellen en uit te dragen (gedragsregels voor privacy en gegevensverwerking);
- privacypolicies te stimuleren (clean desk, clean screen policy);
- procedures toe te passen (meldingen en afhandelingen van incidenten, inbreuken, verzoeken);
- online awareness training.

Verslag aan managers

Daarnaast zorgen we dat de managers op de hoogte zijn van de AVG. Zo maken wij het hen mogelijk de impact van de AVG op hun bestaande processen, diensten en goederen in te schatten en daarop de juiste maatregelen te nemen.

De managers zorgt voor voldoende bewustwording bij hun medewerkers op het gebied van privacy, security en gegevensbescherming. Medewerkers moeten minimaal op de hoogte zijn van de privacyregels en de relevante bepalingen voor hun werkzaamheden zodat zij de ze in hun dagelijkse werk kunnen toepassen. De verantwoordelijkheid voor bewustwording ligt bij de afdelingen. Het team Informatieveiligheid & Privacy kan de afdelingen hierin ondersteunen.

5.4 Verantwoordingsplicht

5.4.1 Verantwoordingsplicht en verplichtingen AVG

Onze verantwoordingsplicht brengt met zich mee dat wij de regels moeten naleven én dat wij dit ook kunnen aantonen. Daarvoor nemen wij deze maatregelen:

- wij houden een register van verwerkingen bij en de afdelingen zorgen dat dit actueel is en blijft;
- als dit noodzakelijk is worden er DPIA's uitgevoerd;
- centraal houden wij een register van datalekken bij die zijn opgetreden, ook als wij die niet hebben gemeld aan de Autoriteit Persoonsgegevens;
- een afdeling of team kan aantonen of iemand toestemming heeft gegeven. Dit is alleen nodig als toestemming de grondslag is voor het werken met de persoonsgegevens;
- wij hebben een FG aangesteld die voldoende middelen heeft om het werk te doen.

Naast bovenstaande maatregelen gelden deze uitgangspunten:

- Wij sluiten overeenkomsten met samenwerkingspartners (als er een gezamenlijke verantwoordelijkheid is voor het verwerken van de gegevens) en verwerkingsovereenkomsten met onze verwerkers waarin wij specifieke afspraken maken over privacy. Deze afspraken kunnen ook in een convenant vastgelegd zijn.
- Wij respecteren de rechten van betrokkenen en zijn transparant richting degene van wie de gegevens zijn over het gebruik van de gegevens (informatieplicht).
- Wij zorgen voor een grondslag en de organisatie houdt zich aan de privacy-beginselen, zoals een rechtsgeldige grondslag, doelbinding, proportionaliteit, juistheid en noodzakelijkheid.
- Wij zorgen ervoor dat de gegevens op een passend niveau beveiligd zijn.
- Wij toetsen periodiek of registers, DPIA's en privacy-overeenkomsten nog voldoen aan de wettelijke verplichtingen en passen deze aan als dat nodig is.
- Wij verwerken in beginsel geen persoonsgegevens buiten de EU/EEG.

5.4.2 Register van verwerkingen

Wij houden een register bij van verwerkingen. Het management zorgt voor de inschrijving van de verwerkingen van persoonsgegevens binnen de afdeling. De proceseigenaren staan het management hierin bij. In het verwerkingsregister worden in ieder geval de volgende gegevens vermeld:

- de naam van de verwerking
- wie de verantwoordelijke is voor de verwerking
- het doel van de verwerking
- de groep van personen van wie wij persoonsgegevens verwerken (betrokkenen)
- de categorieën persoonsgegevens die wij bij de verwerking gebruiken
- de ontvangers van de gegevens
- de rechtmatige grondslag voor de verwerking van de persoonsgegevens
- eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte
- de verwijderingstermijnen die wij in acht nemen.

De FG houdt toezicht op de volledigheid en rechtmatigheid van de verwerkingen van persoonsgegevens die in het register ingeschreven staan en de daarbij behorende documenten (zoals de verwerkingsovereenkomst, DPIA en pre-DPIA). Als wij de processen wijzigen, dan zorgt het management dat de wijziging hiervan in het register wordt doorgevoerd, overeenkomstig het proces. Het management toetst de compleetheid van het register periodiek.

6 Datalekken

Wij hebben op grond van de AVG de plicht om datalekken te melden bij de Autoriteit Persoonsgegevens. Als we een datalek vermoeden of als een datalek is ontdekt, moet direct een melding worden gemaakt bij de Privacy Officer, de FG en de CISO. Daardoor kunnen we zo snel mogelijk acties ondernemen om de melding te registeren, te onderzoeken en af te handelen en zo de rechten en vrijheden van betrokkenen te beschermen. Dit hoofdstuk beschrijft het beleid van de melding, registratie en afhandeling van een datalek of het vermoeden van een datalek binnen SamenTwente.

6.1 Datalek

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot en/of ongeoorloofde of onbedoelde verlies, vernietiging, wijziging en verstrekking van de persoonsgegevens, zoals:

- diefstal van een laptop of een mobiel met persoonsgegevens die bij de werkzaamheden voor SamenTwente worden verwerkt;
- een e-mail met persoonsgegevens versturen naar een verkeerde ontvanger
- verlies van een USB-stick;
- het (on)bedoeld wissen of vernietigen van persoonsgegevens;
- besmetting met ransomware waardoor persoonsgegevens ontoegankelijk zijn
- toegang van een ongeautoriseerde persoon tot persoonsgegevens;
- inzien door een geautoriseerd persoon van gegevens die niet nodig zijn voor de uitvoering van de werkzaamheden.

Meer informatie over datalekken vind je op de website van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekkentfwat-is-een-datalek-precies-5916

De AVG kent de term 'datalek' niet. De AVG spreekt in dit geval van 'een inbreuk in verband met persoonsgegevens'. In het maatschappelijk verkeer hanteren wij de term 'datalek'. leder vastgesteld datalek of ieder vermoeden van een datalek wordt door de SamenTwente gedocumenteerd.

Wij beschouwen als datalek:

- *Inbreuk op de vertrouwelijkheid*: als er ongeoorloofd of onbedoeld toegang is tot persoonsgegevens of wij deze verstrekken.
- *Inbreuk op de integriteit*: als wij ongeoorloofd of onopzettelijk persoonsgegevens wijzigen.
- *Inbreuk op de beschikbaarheid*: als wij (on)opzettelijk of ongeoorloofd toegang tot persoonsgegevens verliezen of (on)opzettelijk of ongeoorloofd persoonsgegevens vernietigen.

6.1.1 Datalekprocedure

Wij melden een vermoeden van een datalek of een datalek direct volgens de datalekprocedure SamenTwente. Alleen op deze wijze kunnen wij het datalek tijdig onderzoeken en indien nodig melden aan de Autoriteit Persoonsgegevens en indien nodig aan de betrokkene(n). Wij brengen medewerkers op verschillende manieren op de hoogte over de procedure.

6.2 Melding en registratie

Interne en externe medewerkers kunnen een datalek binnen SamenTwente melden, ook leveranciers en derden buiten SamenTwente van wie de persoonsgegevens binnen SamenTwente mogelijk zijn betrokken bij een datalek. Dit gebeurt via de procedure datalekken en voor leveranciers en derden via de gemaakte afspraken of verschafte informatie. Is er een datalek vastgesteld of vermoed of zijn er waargenomen of verdachte zwakke plekken in systemen of diensten? Dan melden alle medewerkers, ingehuurd personeel en externe gebruikers dit per direct bij de manager dan wel bij de persoon volgens de gemaakte afspraken. Zij melden het vermoedelijke datalek zoals vastgesteld in de procedure datalekken.

6.2.1 Register datalekken

Wij houden elk gemeld (vermoedelijke) datalek en de afhandeling daarvan bij in het Register datalekken van SamenTwente. Dit register bevat zowel de gemelde datalekken als de datalekken die niet gemeld zijn aan de Autoriteit Persoonsgegevens. Hierin is ook vermeld welke maatregelen zijn genomen om de gevolgen te beperken en herhaling te voorkomen. In de triaalrapportage besteden wij aandacht aan de datalekken.

6.3 Afhandeling

Als er een datalek is, handelen wij dit af volgens de datalekprocedure van SamenTwente, de AVG en de beleidsregels *Meldplicht datalekken* van de Autoriteit Persoonsgegevens. Daarmee zorgen we dat de melding van het datalek de juiste personen en uiteindelijk de toezichthouder en betrokkenen op tijd bereikt. Deze beleidsregels vind je hier: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_meldplicht datalekken.pdf

Bij een datalek met een medium tot hoog risico-inschatting, als de betrokkene(n), de bedrijfsprocessen, de financiën of goede naam van SamenTwente ernstig in gevaar zijn, betrekken wij in ieder geval de directeur bij de afhandeling van het gemelde datalek.

6.4 Besluitvorming

Als de beoordeling van het incident leidt tot een meldingswaardig datalek, nemen wij volgens de procedure datalekken een besluit over de verplichting om het datalek te melden aan de Autoriteit Persoonsgegevens en indien nodig ook aan de betrokkene(n). De directeur is verantwoordelijk (responsible & accountable) voor het besluit om al dan niet melding te maken aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) als het datalek een medio tot hoog risico-inschatting heeft gekregen.

6.5 Evaluatie – verbeterplan

Het is voor de organisatie van groot belang om te leren van bestaande datalekken, om de waarschijnlijkheid van toekomstige datalekken te verkleinen en bedrijfsprocessen te verbeteren. Registratie van datalekken, een periodieke rapportage en een verbeterplan daarover horen bij een professionele manier van verwerken van persoonsgegevens. De rapportage over datalekken van persoonsgegevens is daarom een vast onderdeel van de verslaglegging naar het dagelijks bestuur, de directeur en het voor de verwerking verantwoordelijke management. De Functionaris Gegevensbescherming ziet erop toe dat wij het verbeterplan naleven.

7 Rechten van betrokkenen

7.1 Rechten van betrokkenen

Onder de AVG hebben betrokkenen bepaalde rechten waarmee ze de persoonsgegevens kunnen controleren die SamenTwente van hen verwerkt. Een betrokkene kan een verzoek per e-mail indienen bij de verantwoordelijke van de afdeling waar het om gaat. Een betrokkene kan een verzoek ook via een webformulier op de websites van SamenTwente indienen of per brief via de post. Hieronder staat welke rechten van betrokkenen wij binnen het beleid borgen.

7.1.1 Recht op informatie - privacyverklaring

Wij verzamelen gegevens om taken te kunnen uitvoeren. Als dit persoonsgegevens zijn, hebben wij de plicht om betrokkenen te informeren over verwerkingen van hun persoonsgegevens, als ze daar niet al van op de hoogte zijn. Dit gebeurt in de privacyverklaringen die gepubliceerd zijn op de websites van SamenTwente. Daarnaast kunnen afdelingen andere middelen gebruiken, zoals een informatiefolder. Wij mogen persoonsgegevens pas verwerken nadat betrokkenen hierover geïnformeerd zijn. Dit moet gebeuren voordat de verwerking start.

7.1.2 Recht op inzage

Betrokkenen hebben het recht om ons te vragen of wij hun persoonsgegevens verwerken. Als we dit doen, hebben zij het recht op toegang tot (een kopie van) de verwerkte persoonsgegevens. Hierbij houden wij rekening met de beperkingen zoals staan in wet- en regelgeving. Als een verzoek binnenkomt, pakken wij dit meteen op in overeenstemming met de procedure *Behandelen verzoeken van betrokkenen*.

7.1.3 Recht op correctie en aanvulling

Betrokkenen hebben het recht om persoonsgegevens te laten corrigeren als deze onjuist of onvolledig zijn. Daarbij houden wij rekening met de beperkingen zoals deze staan in wet- en regelgeving. Dit recht houdt in dat wij onvolledige gegevens mogen aanvullen, met een aanvullende verklaring, zodat de persoonsgegevens compleet en juist zijn.

7.1.4 Recht om vergeten te worden

Het recht om persoonsgegevens te doen verwijderen, ook wel het recht om vergeten te worden, is geen absoluut recht. Betrokkenen hebben het recht om persoonsgegevens te laten verwijderen bij één van de volgende redenen:

- De persoonsgegevens zijn niet langer noodzakelijk voor het doel waarvoor ze oorspronkelijk zijn verzameld of verwerkt.
- Betrokkenen trekken de door hen gegeven toestemming in en er is geen andere wettelijke grondslag voor de verwerking.
- Betrokkenen maken bezwaar tegen de verwerking van hun persoonsgegevens en er zijn geen doorslaggevende legitieme redenen zijn voor de verwerking.
- De verwerking van de persoonsgegevens is onrechtmatig.
- Wij moeten de persoonlijke gegevens wissen om te voldoen aan een wettelijke verplichting.

7.1.5 Recht op beperking van de verwerking

Het recht op beperking houdt in dat wij de persoonsgegevens (tijdelijk en onder voorwaarden) niet mogen verwerken en niet mogen wijzigen, bijvoorbeeld wanneer betrokkenen de juistheid van de gegevens ter discussie stellen. Betrokkenen hebben het recht om de verwerking van hun persoonsgegevens te beperken bij één van de volgende redenen:

- De betrokkene betwist de nauwkeurigheid van persoonsgegevens.
- De verwerking is onrechtmatig en betrokkenen verzetten zich tegen het verwijderen van de persoonsgegevens.
- Wij hebben de persoonsgegevens niet langer nodig.

7.1.6 Recht van bezwaar

Betrokkenen hebben het recht ons te vragen hun persoonsgegevens verder niet meer te gebruiken om redenen die samenhangen met hun specifieke situatie. Wij moeten hieraan voldoen, tenzij er gerechtvaardigde gronden zijn voor de verwerking. Soms kan het ook zijn dat wij het bezwaar noteren in een dossier.

7.1.7 Recht op overdraagbaarheid van gegevens (dataportabiliteit)

Met het recht op overdraagbaarheid van gegevens kunnen de betrokkenen hun persoonlijke gegevens voor hun eigen doeleinden krijgen en hergebruiken voor verschillende diensten, maar dit recht is alleen van toepassing:

- op persoonsgegevens die de betrokkenen verstrekt hebben aan SamenTwente;
- als de verwerking is gebaseerd op toestemming van de betrokkenen of voor de uitvoering van een overeenkomst;
- als de verwerking op een geautomatiseerde wijze wordt uitgevoerd.

Wij zijn vanuit de AVG niet verplicht invulling te geven aan overdraagbaarheid van gegevens als:

- het werkzaamheden zijn in het kader van algemeen belang
- er een openbaar gezag wordt uitgeoefend
- het gezag zijn openbare taken uitoefent of voldoet aan een wettelijke verplichting.

7.1.8 Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profilering

Uitgangspunt in de AVG is, dat er geen geautomatiseerde besluitvorming mag zijn op basis van profilering, als daaraan rechtsgevolgen voor de betrokkene (degene wiens persoonsgegevens het betreft) zijn verbonden of het besluit hem in aanmerkelijke mate treft. Daarbij kunnen wij bijvoorbeeld denken aan de kredietwaardigheid van een persoon. Een ander voorbeeld is het verwerken van sollicitaties via internet zonder menselijke tussenkomst. Wij houden ons aan dit verbod en zorgen altijd voor menselijke tussenkomst bij het nemen van besluiten.

7.1.9 Klachten

Iedereen heeft het recht om bij ons een klacht in te dienen tegen de wijze waarop wij zijn of haar persoonsgegevens verwerken. De FG is het aanspreekpunt binnen SamenTwente over de afhandeling van privacy-klachten en de FG adviseert afdelingen zwaarwegend hoe de klacht af te handelen. De betrokkene kan zijn of haar klacht of een verzoek tot bemiddeling ook indienen bij de Autoriteit Persoonsgegevens.

7.2 Hoe kunnen betrokkenen gebruikmaken van deze rechten?

Om gebruik te maken van bovenstaande rechten kunnen betrokkenen een verzoek indienen. Betrokkene kan dit verzoek zowel per e-mail, via de websites van SamenTwente of per papieren post indienen.

7.2.1 Vaststellen identiteit van persoon die het verzoek indient

Wij nemen een verzoek alleen in behandeling nadat wij de identiteit van de betrokkene hebben vastgesteld. Als wij twijfelen aan de identiteit van de betrokkenen of aan die van degene die namens de betrokkenen een verzoek indient, vragen wij aanvullende informatie om de identiteit vast te stellen. Wij schorten de beslistermijn op tijdens de periode waarin de betreffende betrokkene nalaat gehoor te geven aan het verzoek om de aanvullende informatie te verstrekken.

7.2.2 Beslistermijn

Binnen vier weken beoordelen wij of het verzoek gerechtvaardigd is. Wij laten binnen die termijn weten wat er met het verzoek gaat gebeuren, waaronder of wij de behandeling van het verzoek met twee maanden verlengen als hier een goede reden voor bestaat. De Privacy Officer ondersteunt de afdelingen met de afhandeling van het verzoek, overeenkomstig het werkproces.

Als wij het verzoek niet op tijd opvolgen, delen wij uiterlijk binnen vier weken mee waarom het verzoek zonder gevolg is gebleven, of informeren wij betrokkene dat wij de reactietermijn hebben verlengd. De betrokkenen heeft dan het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP).

Kosten en termijn van reactie
Als iemand ons verzoekt om informatie, dan verstrekken wij alle informatie, communicatie of acties kosteloos aan betrokkenen, tenzij een dergelijk verzoek kennelijk ongegrond of buitensporig is, met name vanwege het herhaalde karakter ervan. Wij hebben in dat geval twee mogelijkheden. Wij kunnen een redelijke vergoeding in rekening brengen, rekening houdend met de administratieve kosten van de communicatie, of het verzoek weigeren. Voorafgaand aan het inwilligen van het verzoek geven wij aan de betrokkene de te berekenen kosten op, zodat de betrokkenen toestemming kunnen geven. Weigeren we het verzoek, dan onderbouwen we het kennelijk ongegronde of buitensporige karakter van het verzoek.

Dit is onze termijn van reactie:
- Binnen een maand informeren we de betrokkenen over het gevolg van het verzoek, zonder onnodige vertraging na ontvangst van het verzoek.
- We kunnen de periode met twee maanden verlengen, rekening houdend met de complexiteit en het aantal verzoeken. Van zo'n verlenging stellen wij de betrokkene in voorkomend geval op de hoogte.
- Als we geen actie ondernemen op het verzoek van de betrokkenen, zullen we dit gemotiveerd kenbaar maken aan de betrokkenen. Dit doen wij zonder onnodige vertraging en uiterlijk binnen een maand, of twee maanden bij een verlenging, na ontvangst van het verzoek. Gelijktijdig informeren we de betrokkenen over de mogelijkheid om een klacht in te dienen bij de Functionaris Gegevensbescherming en/of de Autoriteit Persoonsgegevens.

BIJLAGE – Begrippen die wij hanteren

In dit privacybeleid gebruiken wij een aantal begrippen regelmatig. Hieronder leggen wij deze begrippen uit, zodat duidelijk is wat wij met deze begrippen bedoelen.

Wat en over wie?

1. **Persoonsgegevens**

Onder persoonsgegevens verstaan wij alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is. Een natuurlijke persoon kunnen wij onder andere identificeren met een naam, een identificatienummer, locatiegegevens, een online identificator of via een of meer kenmerken van de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals lengte, haarkleur, afkomst en politieke voorkeuren of een combinatie van persoonsgegevens. Als iemand door een combinatie van gegevens kan worden herkend, dan geldt elk van deze gegevens als een persoonsgegeven. Een voorbeeld is een functie binnen een organisatie of een cliëntnummer in een dataset.

2. **Betrokkene**

De betrokkene is de geïdentificeerde of identificeerbare natuurlijke persoon op wie de verwerkte en/of de te verwerken persoonsgegevens betrekking hebben. Dit betekent dat de betrokkene de persoon is van wie wij de persoonsgegevens verwerken.

3. **Verwerking**

Bijna alles wat wij met persoonsgegevens doen is een verwerking. Onder een (geheel van) verwerking(en) valt elke activiteit van vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken met doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van persoonsgegevens.

Door wie/ welke rollen?

4. **Verwerkingsverantwoordelijke**

Een partij die belast is met het uitvoeren van een wettelijke taak is verwerkings-verantwoordelijk voor de omgang met de persoonsgegevens. Geeft deze persoon een taak door via een gemeenschappelijke regeling, dan gaat ook de verwerkings-verantwoordelijkheid mee over. Bij mandaat ligt dit anders: soms wijst de wet een minister aan als verwerkingsverantwoordelijke, bijvoorbeeld voor een landelijk schakelpunt.

Daarnaast is de partij (mede)verwerkingsverantwoordelijk die, zelf of samen met anderen, de doeleinden en middelen voor de verwerking van persoonsgegevens bepaalt. Hiermee bedoelen we de partij die voor de verwerking bijvoorbeeld bepaalt:

- welke gegevens
- met welk doel
- wie toegang heeft
- wie de gegevens opslaat en hoe lang
- wie de gegevens verwijdert en/of wij de gegevens teruggeven.

5. Gezamenlijke verwerkingsverantwoordelijke(n)

Dit zijn de partijen die samen een wettelijke taak uitvoeren en/of de doeleinden en de middelen voor de verwerking van persoonsgegevens bepalen. In welke fase en in welke mate een partij verwerkingsverantwoordelijk is, kan verschillen. Belangrijkste doel van het benoemen van de gezamenlijkheid is te voorkomen dat de betrokkene via elke partij zijn privacy rechten kan uitoefenen.

6. Verwerker

De verwerker is de partij die persoonsgegevens alleen verwerkt in opdracht van een verwerkingsverantwoordelijke. De verwerker is een rechtspersoon en deze handelt niet onder het gezag van de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke sluit met de verwerker een verwerkingsovereenkomst waarin zij de afspraken vastleggen over de geheimhouding en de beveiligingsmaatregelen die de verwerker neemt.

7. Derde

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, die niet tot één van de volgende groepen behoort:

- betrokkene, (gezamenlijke) verwerkingsverantwoordelijke of verwerker
- personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken

Dit betekent dat een derde niet rechtstreeks betrokken is bij de verwerking van de persoonsgegevens, maar wel op een bepaalde manier kennis kan nemen van die persoonsgegevens. Denk bijvoorbeeld aan:

- politie
- samenwerkingspartners
- belastingdienst
- burgemeester

Enkele AVG-instrumenten

8. Datalekken

Heeft iemand toegang tot persoonsgegevens of vernietiging, verlies, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van de organisatie? Dan noemen we dat een datalek. Voorbeelden zijn:

- diefstal van laptop/ mobiele telefoon of verlies van een usb-stick of notitieboekje
- als een medewerker onrechtmatig gegevens inziet en/of foto's of screenshots maakt
- als een medewerker een brief naar een onjuist adres verstuurt
- als een medewerker onbedoeld bestanden verwijdert

9. Privacy by default (gegevensbescherming door standaardinstellingen)

Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn dat wij de privacy van betrokkenen maximaal waarborgen. Dit betekent onder meer dat we zo min mogelijk persoonsgegevens vragen en verwerken. Aan de betrokkene vragen we expliciet om in te stemmen met het verwerken van meer persoonsgegevens (opt-in).

10. Privacy by design (gegevensbescherming door ontwerp)

Bij de ontwikkeling van producten en diensten houden wij voor de gehele levenscyclus van persoonsgegevens zoveel mogelijk rekening met de privacy van betrokkenen. Dit is vanaf het verzamelen tot het verwerken en verwijderen van de gegevens. Hierbij passen we stelselmatig privacy verhogende maatregelen en technieken toe, bijvoorbeeld voor de nauwkeurigheid, verantwoordelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.

11. Data Protection Impact Assessment (DPIA)

Een DPIA is een instrument waarmee we de privacyaspecten van een verwerkingsactiviteit helder en gestructureerd in beeld brengen en de risico's voor de betrokkenen ook. Met de DPIA kunnen wij de geïdentificeerde risico's beperken tot een aanvaardbaar niveau, doordat de DPIA maatregelen voorstelt die we kunnen uitvoeren.