Informatiebeheerbeleid

(inclusief privacyreglement en meldplicht datalekken)

Inhoudsopgave

Voorwoord

Waarom een informatiebeheerbeleid?

Stichting Omega is een organisatie die veel werkt met persoonsgegevens van cliënten en medewerkers. Het is daarom belangrijk om waarde te hechten aan het beschermen van de privacy van de cliënten en medewerkers waar de organisatie mee te maken krijgt. Dit vraagt om een integraal informatiebeheerbeleid waarin rekening gehouden wordt met de bescherming van de persoonsgegevens en het voldoen aan wet –en regelgeving.

De volgende wet-en regelgeving is verankerd in dit informatiebeheerbeleid:

- Algemene verordening gegevensbescherming (AVG)

De AVG stelt de richtlijnen betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het verkeer van deze gegevens. Onder de AVG is het protocol datalekken aangescherpt. Dit protocol verplicht datalekken te melden bij de Autoriteit Persoonsgegevens.

Wat staat er in het informatiebeheerbeleid?

- Verantwoordelijken informatiebeheerbeleid
- Welke informatie in bezit is van Omega
- Hoe de informatie wordt verwerkt en gebruikt
- Waar en hoe de informatie wordt gearchiveerd
- Of er een veiligheidskopie van de betreffende gegevens wordt gemaakt en waar die zich bevindt
- Bewaartermijn en het vernietigen van informatie
- Hoe om te gaan met een klacht/ bezwaar
- Hoe te handelen bij een datalek in het kader van de Meldplicht datalekken

1. Begripsbepalingen

1. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
2. Gezondheidsgegevens: Alle gegevens die de geestelijke of lichamelijke toestand van een cliënt betreffen;
3. Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens;
4. Bestand: Gestructureerd geheel dat betrekking heeft op de persoonsgegevens van de cliënt en dat volgens bepaalde criteria toegankelijk is voor derden;
5. Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
6. Betrokkene: degene op wie een persoonsgegeven betrekking heeft;
7. Verwerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
8. Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
9. Ontvanger: degene aan wie de persoonsgegevens worden verstrekt;
10. Autoriteit Persoonsgegevens; de Autoriteit Persoonsgegevens heeft tot taak toe te zien op de verwerking van persoonsgegevens. Bedrijven, instellingen en overheden die persoonsgegevens verwerken zijn verplicht datalekken te melden bij de Autoriteit Persoonsgegevens (voorheen College Bescherming Persoonsgegevens, het CBP)

2. Reikwijdte

Dit reglement is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

3. Informatie in bezit van Omega

De persoonsregistratie binnen Omega bevat de volgende gegevenscategorieën:
- personalia/ identificatie gegevens
- financieel/ administratieve gegevens
- medische, paramedische en psychologische gegevens (gezondheidsgegevens)
- zorginhoudelijke gegevens

4. Verantwoordelijken informatiebeheerbeleid

4.1. Houder informatiebeheerbeleid
De directeur van Omega is eindverantwoordelijk voor het informatiebeheerbeleid. De directeur is verantwoordelijk voor het goed functioneren van de persoonsregistratie en aansprakelijk voor eventuele schade als gevolg van het niet naleven van dit beleid.

4.2. Functionaris Gegevensbescherming (FG)
Een onafhankelijke medewerker die belast is met het toezicht op de naleving van de AVG. De FG fungeert ook als aanspreekpunt voor de AP, bijvoorbeeld bij een (vermoeden van) datalek.

4.3. Portefeuillehouder
De manager Ondersteunende Diensten is als portefeuillehouder verantwoordelijk voor het informatiemanagement en de naleving van het vastgestelde beleid. De portefeuillehouder is verantwoordelijk voor het goed functioneren van de onder zijn beheer staande faciliteiten, in samenspraak met o.a. de facilitair coördinator. Hij draagt zorg voor de beveiliging tegen verlies en onbevoegde kennisneming, wijziging of verstrekking van gegevens en voor het regelmatig opschonen van de persoonsregistratie.

4.4. Evaluatie beleid
Het informatiebeheerbeleid wordt jaarlijks geëvalueerd en opgenomen in de directiebeoordeling. De directeur en portefeuillehouder zijn hiervoor verantwoordelijk. De informatieveiligheid wordt naar aanleiding van de directiebeoordeling jaarlijks besproken in het MT.

5. Doel van de verwerking van de persoonsgegevens

Stichting Omega neemt alleen de persoonsgegevens op, bewerkt en/of bewaart ze met een bepaald doel. De gegevensverzameling en verwerking moet samenhangen met het vooraf gestelde doel.

Doeleinden voor de verwerking van persoonsgegevens:
- Een goede uitvoering van de zorg-, hulp- en dienstverlening die door Stichting Omega wordt verleend;
- Verantwoording van de zorg-, hulp- en dienstverlening;
- Het vastleggen en beschikbaar stellen van persoonsgegevens voor onderzoek en kwaliteitscontrole;
- Het financieel afhandelen van de geboden zorg aan de cliënt.

Stichting Omega zal geen persoonsgegevens verwerken voor andere dan bovengenoemde doeleinden.

6. Voorwaarden voor de verwerking van de persoonsgegevens

Persoonsgegevens mogen slechts worden verwerkt indien aan een van de voorwaarden is voldaan:
- De betrokkene heeft toestemming verleend;
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst;
- De verwerking is noodzakelijk voor de uitvoering van een wettelijke plicht;

- De verwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;
- De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang;
- Er rekening gehouden is met de wijze waarop de gegevens zijn verkregen.

7. Kennisgeving aan (vertegenwoordiger van de) betrokkene

7.1
Stichting Omega stelt de (vertegenwoordiger van de) betrokkene wiens gegevens voor het eerst zijn opgenomen binnen een maand na opneming van de gegevens op de hoogte en wijst hem op het bestaan van het informatiebeheerbeleid.

7.2.
Stichting Omega zal door middel van een algemene kennisgeving het bestaan van de registratie en van dit beleid vermelden, alsmede daarin aangeven op welke wijze het beleid kan worden ingezien en verkregen en nadere informatie ter zake kan worden ingewonnen.

7.3
Indien andere doeleinden dan genoemd onder paragraaf 5 een doelstelling vormen van de registratie, heeft Stichting Omega de plicht de betrokkene vooraf schriftelijk te informeren omtrent de aard van de gegevens die over zijn persoon in de registratie zijn opgenomen, alsmede omtrent de doeleinden die daarmee worden nagestreefd.

8. Verstrekking van persoonsgegevens

8.1.
Voor verstrekking van persoonsgegevens aan derden is toestemming van de (vertegenwoordiger van de) betrokkene vereist. Deze toestemming is niet vereist indien verstrekking noodzakelijk is ter uitvoering van een wettelijke plicht of een andere voorwaarde voor de verwerking van de persoonsgegevens zoals genoemd onder paragraaf 6.

8.2.
Binnen Stichting Omega kunnen zonder toestemming van de betrokkene en indien noodzakelijk voor de taakuitoefening, geregistreerde persoonsgegevens worden verstrekt aan:
- Degenen die rechtstreeks betrokken zijn bij de actuele zorgverlening aan de betrokkene;
- Degenen die betrokken zijn bij kwaliteitsdoelstellingen (interne auditteam).

8.3.
Buiten Stichting Omega kunnen zonder toestemming van de betrokkene en indien noodzakelijk voor de taakuitvoering van Omega, geregistreerde persoonsgegevens worden verstrekt aan:
- Personen en instanties, wier taak het is verleende zorg te controleren en toetsen;
- Zorgverzekeraars;
- Certificeringinstanties (TUV);
- Organen zoals CIZ, WLZ en aan het ministerie van VWS;
- Inspectie voor de Volksgezondheid.

9. Beveiliging van de persoonsgegevens

De persoonsregistratie binnen Omega vindt geschreven of digitaal plaats en wordt bewaard in een persoonsgebonden (papieren) dossier dan wel in een persoonsgebonden dossier op het netwerk van Omega. In het kader van de zorg kunnen audiovisuele opnamen gemaakt worden van een betrokkene.

9.1 Toegang tot en gebruik van persoonsgegevens
Onverminderd eventuele wettelijke voorschriften te zake hebben slechts toegang tot de persoonsgegevens:
- De bewerker die deze gegevens heeft verzameld of diens waarnemer.
- Andere direct bij de verzorging, begeleiding en/ of behandeling betrokken beroepsbeoefenaren voor zover de taakuitoefening noodzakelijk.
- De directeur en de bewerker, voor zover dit in het kader van beheer en bewerking noodzakelijk is.

9.2 Beveiliging digitale dossiers
Toegang en bewerken van de digitale persoonsgegevens is geregeld door het autoriseren van de toegang en het verlenen van rechten om de informatie in te zien danwel te bewerken.

9.3 Autorisatie
Er zijn per medewerker gebruikersrechten toegekend voor het gebruik van software van de organisatie door middel van een wachtwoord (en token). Het wachtwoord is persoonsgebonden en mag niet worden doorgegeven. Medewerkers mogen alleen die persoonsgegevens inzien die voor hun taakuitoefening noodzakelijk zijn.

9.4 Beveiliging papieren dossiers
De papieren dossiers zijn binnen Omega ondergebracht in een afgesloten dossierkast of in het archief.
Op de groepen is een onderdeel van de persoonsregistratie aanwezig welke noodzakelijk is voor de dagelijkse zorg aan de betrokkene. Deze gegevens zitten in persoonsgebonden mappen, welke worden opgeborgen in een afgesloten kast/ruimte op de groep. Indien op de groepen gebruik wordt gemaakt van werkdocumenten (waaronder bijv werkdoelen), mogen deze buiten de mappen op de groep bewaard worden, mits de persoonsgegevens niet zichtbaar zijn (met uitzondering van de naam).

9.5 Bewaren en gebruiken van beeld –en geluidsmateriaal
De afspraken hierover zijn vastgelegd in het beleid beeld- en geluidsmateriaal.

9.6 Back-up regeling
De back-up van alle gegevens op de server van Stichting Omega:
- Een onsite back-up via de NAS.
- Een offsite back-up via Constant – IT.

De back-up van alle gegevens in Qsuite (Novire):
- Bij Novire worden dagelijks twee kopieën gemaakt van alle documenten op alle shares (schijven). Daarnaast worden er elke dag back-ups gemaakt van alle servers.

- Stichting Omega heeft een overeenkomst (Escrow-regeling) afgesloten met de Software Borg Stichting. De broncode van door Stichting Omega gebruikte software is opgeslagen bij een IT notaris.

10. Bewaartermijn van de persoonsgegevens

10.1
De directeur van Omega heeft besloten alle papieren en digitale dossiers te bewaren met als motivatie 'de uniekheid van de doelgroep'. Omega bewaart de geanonimiseerde persoonsgegevens voor wetenschappelijke doeleinden.
Voor de persoonsgegevens die niet zijn opgenomen in de papieren en digitale dossiers geldt een bewaartermijn van in beginsel 15 jaren, te rekenen vanaf het tijdstip waarop de gegevens zijn vervaardigd, of zoveel langer als redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit.

10.2.
Indien de bewaartermijn van de persoonsgegevens (die niet zijn opgenomen in de papieren en digitale dossiers) is verstreken, worden de desbetreffende persoonsgegevens uit de registratie vernietigd, zulks binnen een termijn van één jaar.
Vernietiging blijft evenwel achterwege indien:
- daarover tussen de (vertegenwoordiger van de) betrokkene en de bewerker overeenstemming bestaat.
- Indien de betreffende gegevens zodanig zijn bewerkt, dat herleiding tot individuele personen redelijkerwijs onmogelijk is. In dit geval kunnen de gegevens in geanonimiseerde vorm bewaard blijven.

11. Aanvulling, correctie of vernietiging van persoonsgegevens

11.1.
Op verzoek van de (vertegenwoordiger van de) betrokkene vult de bewerker de opgenomen gegevens aan met de door de (vertegenwoordiger van de) betrokkene gewenste aanvullende gegevens. De (vertegenwoordiger van de) betrokkene kan aan de bewerker van de persoonsregistratie een verklaring afgeven met betrekking tot de opgenomen gegevens; deze verklaring wordt opgenomen in het persoonsdossier.

11.2.
De (vertegenwoordiger van de) betrokkene kan Stichting Omega schriftelijk, gemotiveerd, verzoeken om correctie van op de betrokkene betrekking hebbende gegevens, indien deze
- feitelijk onjuist zijn;
- voor het doel van de registratie onvolledig of niet ter zake dienend zijn;
- in strijd met een wettelijk voorschrift in de registratie voorkomen.

11.3.
De (vertegenwoordiger van de) betrokkene kan Stichting Omega schriftelijk verzoeken om vernietiging van tot zijn persoon herleidbare gegevens.

11.4.
Stichting Omega beslist niet over een verzoek in 11.2 en 11.3, dan na de bewerker die de gegevens heeft verzameld of diens opvolger, te hebben gehoord. Stichting Omega deelt haar

beslissing binnen acht weken na ontvangst van het verzoek tot correctie of vernietiging schriftelijk aan de (vertegenwoordiger van de) betrokkene mee. Een weigering is met redenen omkleed.

11.5. Stichting Omega draagt zorg dat een beslissing tot correctie zo spoedig mogelijk wordt uitgevoerd.

11.6. Stichting Omega draagt zorg voor vernietiging van de gegevens zonder onredelijke vertraging na een daartoe strekkend verzoek van de (vertegenwoordiger van de) betrokkene, tenzij

- redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan de geregistreerde, alsmede;
- bewaring op grond van een wettelijk voorschrift vereist is.

11.7. Stichting Omega doet aan degenen, aan wie zij in het haar voorafgaand aan het verzoek en sinds dat verzoek verstreken perioden, gegevens heeft verstrekt, mededeling van de aanvulling, correctie of vernietiging.

11.8. Stichting Omega doet aan de (vertegenwoordiger van de) betrokkene opgave van degene aan wie zij mededeling als bedoeld in 10.7. heeft gedaan, tenzij de (vertegenwoordiger van de) betrokkene te kennen heeft gegeven op de mededeling geen prijs te stellen.

12. Inzage en afschrift van de persoonsgegevens

12.1.
De (vertegenwoordiger van de) betrokkene heeft het recht kennis te nemen van de op de betrokkene betrekking hebbende geregistreerde gegevens en hiervan een afschrift te ontvangen. Hiertoe kan een (schriftelijk) verzoek worden ingediend bij Stichting Omega.

12.2.
De gevraagde inzage en/ of het gevraagde afschrift zal zo spoedig mogelijk, doch uiterlijk binnen vier weken, plaatsvinden respectievelijk worden verstrekt.

12.3.
De gevraagde inzage en/ of het gevraagde afschrift kan worden geweigerd als daarmee gewichtige belangen van een andere dan de verzoeker worden geschaad. Het kan belangrijk zijn dat in de persoonsregistratie opgenomen gegevens van derden vertrouwelijk blijven.

13. Overdracht van opgenomen persoonsgegevens.

13.1.
De (vertegenwoordiger van de) betrokkene heeft het recht op de betrokkene betrekking hebbende gegevens te doen overdragen aan een andere, door hem aan te wijzen houder. Daartoe dient hij een schriftelijk verzoek in bij Stichting Omega. De inwilliging van dit verzoek kan slechts worden geweigerd op grond van een wettelijk voorschrift dan wel worden opgeschort voor zover Stichting Omega jegens de financier van de verleende diensten tot bewaring gehouden is of indien ter zake van die dienstverlening een geschil aanhangig is gemaakt of dreigt te worden gemaakt.

13.2.
In geval Stichting Omega het voornemen heeft tot overdracht van de door haar gehouden persoonsgegevens in verband met beëindiging of wijziging van de juridische status van de instelling, dient Stichting Omega door middel van een (herhaaldelijke) advertentie in een of meer regionale kranten of een maatregel van gelijke strekking, de (vertegenwoordiger van de) betrokkene over de voorgenomen overdracht te informeren, opdat deze voldoende kans wordt geboden tegen het voornemen bezwaar te maken.

14. Looptijd van de registratie

Onverminderd eventuele wettelijke bepalingen is dit beleid van kracht gedurende de gehele looptijd van de registraties.

15. Klachten

15.1.
Indien de (vertegenwoordiger van de) betrokkene van mening is dat de bepalingen van dit reglement niet worden nageleefd of andere reden heeft tot klagen met betrekking tot de registratie van zijn gegevens, dient hij zich te wenden tot Stichting Omega.

15.2.
Indien dit voor de (vertegenwoordiger van de) betrokkene niet leidt tot een voor hem acceptabel resultaat heeft hij de volgende mogelijkheden:
- Zich richten tot de Functionaris Gegevensbescherming van Stichting Omega, bereikbaar via FG@stichtingomega.nl
- Gebruik maken van de klachtenregeling van Omega.
- Zich wenden tot de Autoriteit Persoonsgegevens met het verzoek te bemiddelen of te adviseren in zijn geschil met Stichting Omega. Dit dient te geschieden binnen een termijn van acht weken na ontvangst van het antwoord van Stichting Omega of, indien Stichting Omega niet binnen de gestelde termijn heeft geantwoord binnen acht weken na afloop van die termijn.

Eén en ander laat onverlet de mogelijkheden een beroep te doen op de rechter, hiervoor geldt dezelfde termijn als voor het inschakelen van de Autoriteit Persoonsgegevens.

16. Vaststelling en wijzigingen van het informatiebeheerbeleid

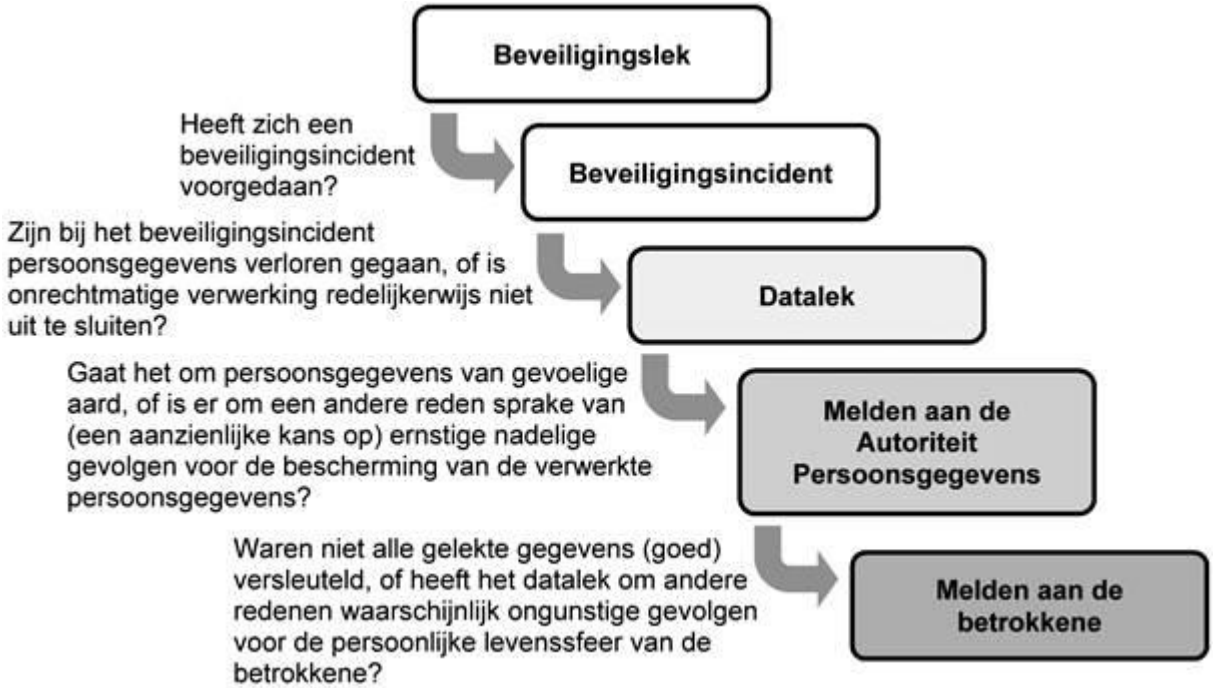
Dit informatiebeheerbeleid wordt vastgesteld door de directeur.
Wijzigingen in dit beleid worden aangebracht door de directeur. De wijzigingen in het beleid zijn van kracht vier weken nadat ze bekend zijn gemaakt aan belanghebbenden.

17. Meldplicht datalekken

Vanaf 1 januari 2016 is de Meldplicht datalekken van toepassing. De meldplicht datalekken houdt in dat de organisatie de Autoriteit persoonsgegevens direct in kennis moet stellen van een datalek of een inbreuk op de beveiliging, die ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens of leidt tot een aanzienlijke kans daarop.
De meldingsplicht binnen de meldplicht datalekken is ruim en het is de toezichthouder van de Autoriteit Persoonsgegevens die de afweging maakt of het datalek ernstig is. Dat doet de autoriteit door te kijken naar de hoeveelheid en de gevoeligheid van de betreffende gegevens. Het nalaten van melding van een datalek wordt beboet met een bestuurlijke boete.

17.1 Beveiligingsincident en datalek
Een beveiligingsincident is volgens de wet het verlies of de onrechtmatige verwerking van gegevens, die eventueel nadelige gevolgen kunnen hebben voor de bescherming van die gegevens. Dat kan dus ook dataverlies betreffen waarbij een actuele of complete veiligheidskopie ontbreekt, zonder dat er gerede kans bestaat dat een derde die data in handen heeft gekregen.
Niet ieder beveiligingsincident is ook een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatige verwerking van de persoonsgegevens niet redelijkerwijs kunt uitsluiten.
Alleen als er sprake is van een datalek moet er melding gedaan worden bij de Autoriteit Persoonsgegevens. Zie figuur 1.

Figuur 1



18. Hoe te handelen bij een beveiligingsincident

18.1
Wanneer een beveiligingsincident wordt ontdekt, is het van belang hier zo snel mogelijk melding van te maken. Dit wordt gedaan door een melding informatiebeveiliging in te vullen in Qsuite. Deze melding komt bij de manager Ondersteunende Diensten terecht. De manager neemt direct telefonisch contact op met de FG. De FG beoordeelt of er sprake is van een datalek en of de Autoriteit Persoonsgegevens geïnformeerd moet worden. De directeur en, indien noodzakelijk, andere betrokkenen worden over de melding geïnformeerd.

18.2
Het datalek wordt uiterlijk binnen 72 uur gemeld via het online 'meldloket datalekken' van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens stuurt een ontvangstbevestiging dat het datalek gemeld is.
Via het meldloket kan de melding tevens aangevuld of ingetrokken worden.

18.3
De Autoriteit Persoonsgegevens neemt contact op met de FG wanneer de melding aanleiding is voor nader te ondernemen activiteiten.

18.4
Indien de FG oordeelt dat er geen sprake is van een datalek, wordt de informatie uit het 'meldingsformulier informatiebeveiliging' meegenomen in de kwartaalanalyse van de FG.

19. Overig
Over zaken waarin dit informatiebeheerbeleid geen uitsluitsel verschaft, beslist de directeur.