Broeders van Liefde
ONDERWIJS EN ZORG

STRATEGISCH BELEID | versie januari 2024 | Goedgekeurd op de CSGGB[1] 30/01/2024 en bekrachtigd op de Bestuursorganen van de vzw Organisatie Broeders van Liefde op xx/xx/2024, de vzw Asster op xx/xx/2024, en ASBL Oeuvres des Frères de la Charité op xx/xx/2024.
Revisie: januari 2028 op de CSGGB
DPO-office: Rinaldo Vereecken en An Theunis

Strategisch Informatiebeveiligingsbeleid[2]

Voor de vzw Organisatie Broeders van Liefde, de vzw Asster en de ASBL Oeuvres des Frères de la Charité[3]

Inhoud

1 Voorwoord 2
2 Beleidsverklaring 3
2.1 Inleiding 3
2.2 Doelstellingen 4
2.3 Toepassingsgebied 4
3 Visie 5
3.1 Kwaliteit 5
3.2 Regelgeving en ethiek 5
3.3 Een lerende organisatie 5
3.4 Realisme 5
4 Het managementsysteem voor informatiebeveiliging 6
4.1 Bewustwording en training 6
4.2 Managementsysteem informatiebeveiliging 6
4.3 Ondersteunende documentatie 7
4.4 Monitoring en evaluatie 8
5 Rollen en verantwoordelijkheden 8
5.1 Medewerkers van de Groep Broeders van Liefde 8
5.2 Bestuursorganen 8
5.3 Lokale directie 9
5.4 Centrale Stuurgroep Gegevensbescherming 9
5.5 Functionaris voor gegevensbescherming 9
5.6 Lokale DPO's/aanspreekpersonen 9
5.7 Team ICT 9

[1] CSGGB: 'Centrale Stuurgroep Gegevensbescherming'.
[2] Zie art. 24, lid 2 GDPR | De aspecten rond privacy worden in een apart beleidsdocument uitgewerkt, alhoewel beide begrippen sterk met elkaar verbonden zijn.
[3] Als in deze tekst 'Groep Broeders van Liefde' staat, verwijzen we steeds naar de drie vzw's zoals hier gedefinieerd.

1 Voorwoord

Door de voortdurende digitalisering, de toenemende cybercriminaliteit en de continue veranderende wet- en regelgeving is het belangrijk dat we zorgvuldig omgaan met data en informatie en ons bewust zijn van onze acties. Immers binnen de Groep Broeders van Liefde wordt continu gevoelige informatie verzameld, beheerd en verwerkt over cliënten[4], medewerkers[5], leveranciers[6] en aangeleverde diensten vanuit haar wettelijke opdracht. Een opdracht met tevens een wettelijke verplichting tot adequate beveiliging. Het bestuur van de Groep Broeders van Liefde erkent dat informatie en de systemen om die informatie te verwerken, waardevolle activa zijn die essentieel zijn voor de Groep Broeders van Liefde. Het is belangrijk om deze informatie te beschermen tegen interne en externe bedreigingen. Een effectief informatiebeveiligingsbeheer is van cruciaal belang om de voortzetting van de Groep Broeders van Liefde en hun diensten te garanderen.

Het informatiebeveiligingsbeleid bestaat enerzijds uit een strategisch beleid en anderzijds uit een operationeel beleid. Het strategisch beleid verwijst naar de overkoepelende strategie en het beleid om de informatiebeveiliging binnen de Groep Broeders van Liefde te waarborgen. Dit beleid is essentieel om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen en om de organisatie te beschermen tegen verschillende bedreigingen, zoals cyberaanvallen, datalekken en andere beveiligingsrisico's. Het operationeel informatiebeveiligingsbeleid is de afgeleide van het strategisch beleid en heeft betrekking op de dagelijkse operationele aspecten van informatiebeveiliging binnen de Groep Broeders van Liefde. Het operationeel beleid vertaalt de brede doelstellingen en principes van het strategische beleid naar concrete maatregelen en procedures die op operationeel niveau worden nageleefd.

[4] Om de leesbaarheid te verhogen wordt er voor gekozen om in dit beleid de term cliënt(en) te gebruiken. Met cliënt verwijzen we naar de patiënt, de bewoner, de zorgvrager, de cliënt, de leerling, de student, de jongere, ouders, (wettelijk) vertegenwoordiger(s), netwerken… M.a.w. die personen waarvoor onze Groep opkomt.

[5] Met medewerkers verwijzen we naar de collega's die werkzaam zijn in de zorg, artsen, medewerkers uit ondersteunde diensten, onderwijspersoneel, vrijwilligers… dit zowel in de lokale voorzieningen als op de centrale diensten.

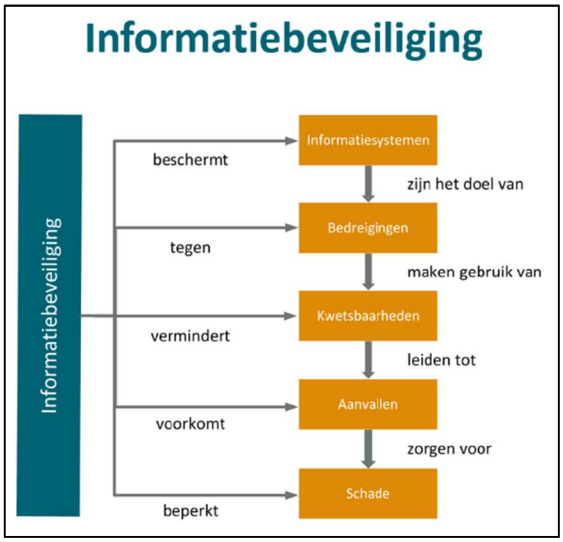
[6] Leveranciers zijn firma's, en hun medewerkers, die ofwel diensten leveren ofwel software/hardware.

2 Beleidsverklaring

2.1 Inleiding

Het strategisch beveiligingsbeleid definieert het hoger kader voor het beheer van informatiebeveiliging binnen de Groep Broeders van Liefde. Het beleid gaat niet alleen over technische maatregelen, cybersecurity en datalekken maar ook over awareness, of hoe kunnen we gedrag beïnvloeden om bewuster om te gaan met data en informatie.

De directe (ofwel primaire) processen rond de dagelijkse werking in de voorzieningen en de indirecte (ofwel de ondersteunende) processen (zowel lokaal als centraal) van onze organisatie zijn sterk afhankelijk van het goed functioneren van informatie. Een uitval, beschadiging of onbevoegd gebruik van informatie kan grote gevolgen hebben. Ongestoorde voortgang van werkzaamheden is belangrijk.



Het doel van dit beleid is het vaststellen van de kaders waarbinnen het 'Information Security Management System' (ISMS) voor informatiebeveiliging binnen de Groep Broeders van Liefde is ingericht en hoe de beveiliging van informatie gewaarborgd wordt. Om dit beleid vorm te geven wordt, naast de wet en regelgeving, gebruik gemaakt van de ISO[7] 27K normering en NIS-2[8] en het CyberFundamentals Framework[9]. Een duidelijk kader waarin beveiligingsbeheersmaatregelen zijn opgesomd die een kapstok aanbieden voor de uitwerking van het jaaractieplan. Het strategisch beleid wordt uitgeschreven voor vier jaar, het operationeel beleidsplan zal jaarlijks gereviseerd worden en vertaald in jaaractieplannen die SMART geformuleerd worden, of Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden.

[7] De norm ISO/IEC 27001 is een uitgave van ISO ('International Organization for Standardization') en IEC ('International Electrotechnical Commission').

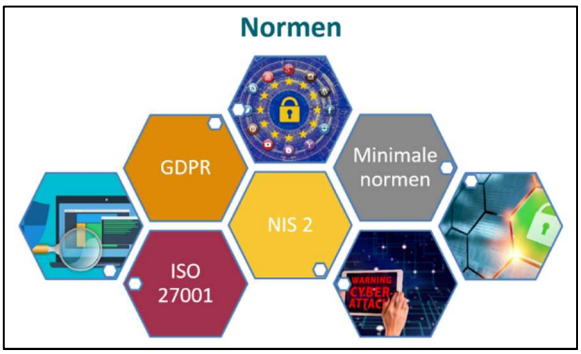
[8] NIS2 = 'Network and Information Systems 2' 'Netwerk en InformatieSystemen' (Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148).).

[9] Voor meer details wordt verwezen naar de website: https://atwork.safeonweb.be/nl/tools-resources/cyberfundamentals-framework waar omschreven staat dat: "*Het CyberFundamentals Framework is een reeks concrete maatregelen om: gegevens te beschermen, het risico op de meest voorkomende cyberaanvallen aanzienlijk te verminderen, de cyberweerbaarheid van een organisatie te vergroten.*" overgenomen op 15/02/2024.

2.2 Doelstellingen

Het informatiebeveiligingsbeleid tracht rekening te houden met alle mogelijke aspecten die voor onze Groep Broeders van Liefde een gevaar kunnen vormen of schade kunnen veroorzaken. Al deze risico's worden in kaart gebracht en bestudeerd op basis van de ISO27k beheersmaatregelen, waarna de passende acties worden gekozen.

Met dit informatiebeveiligingsbeleid willen we compliant zijn aan de Belgische en Europese wetgeving. Zoals de Algemene Verordening Gegevensbescherming[10], maar ook aan de NIS-2 en de minimale normen (ISO27k). Tevens is er een verbinding met de Ziekenhuis- en Onderwijswetgeving, de Kwaliteitswet en de Wet op de Patiëntenrechten.



Het doel van informatiebeveiliging is het waarborgen van de continuïteit van de primaire en ondersteunende processen en diensten binnen de Groep Broeders van Liefde. Het is dan ook belangrijk dat we alle fysieke en elektronische activa benaderen vanuit de CIA-principes (Confidentiality, Integrity and Availability): vertrouwelijkheid, integriteit en beschikbaarheid. Elke letter (CIA) vertegenwoordigt een belangrijk principe in informatiebeveiliging. Deze principes kunnen omgezet worden in volgende vragen:

- Vertrouwelijkheid: zijn de gegevens enkel beschikbaar voor bevoegde personen?
- Integriteit: zijn de gegevens correct en up-to-date en zijn ze enkel door bevoegde personen gemaakt of aangepast?
- Beschikbaarheid: kunnen we de gegevens gebruiken op het moment dat we ze nodig hebben?

Daarom dient de informatie vindbaar, toegankelijk, uitwisselbaar en herbruikbaar te zijn (cf. de FAIR-principes: Findable, Accessible, Interoperable and Reusable). De data dienen immers tijdig beschikbaar, correct en volledig te zijn als essentieel onderdeel voor de veiligheid van cliënten en medewerkers en voor het vervullen van taken en behalen van doelstellingen.

2.3 Toepassingsgebied

Het beleid is enerzijds bedoeld voor medewerkers, voor tijdelijk tewerkgestelde medewerkers (o.a. stagiairs, vrijwilligers en interims), en personen die door medewerkers worden ingezet om diensten te verlenen aan een voorziening van de Groep Broeders van Liefde en haar vzw's. En anderzijds de partners in de meest brede zin van het woord, ongeacht tijdstip, gebruikte apparatuur en locatie.

Het beleid is ook van toepassing op alle data die, al dan niet gestructureerd, informatie wordt, maar ook op de ontwikkelde, operationele én te ontwikkelen systemen, inclusief de informatie die deze systemen kunnen bevatten. Daarnaast is ook de fysieke toegangsbeveiliging van primordiaal belang om de activa daadwerkelijk te kunnen beveiligen.

[10] 'Algemene verordening gegevensbescherming (AVG)' of 'Règlement général sur la protection des données (RGPD)' of 'General Data Protection Regulation (GDPR)'.

3 Visie

3.1 Kwaliteit

De Groep Broeders Van Liefde wil kwalitatieve diensten leveren in de verschillende sectoren en dit informatiebeveiligingsbeleid maakt integraal deel uit van deze focus op kwaliteit. Dit wil enerzijds zeggen dat de kwaliteit van de dienstverlening in het gedrang komt als de informatiebeveiliging onvoldoende gegarandeerd is en anderzijds dat informatiebeveiliging geen doel op zich is, maar altijd deel uitmaakt van onze focus op de kwaliteit van de werking.

3.2 Regelgeving en ethiek

Het registreren en beheren van persoonsgegevens is strikt gereglementeerd door overheden (zowel de Europese als de Belgische). Wij volgen de bepalingen van de overheden op en engageren ons om bij wijziging van de regelgeving op tijd de nodige aanpassingen door te voeren in de Groep Broeders Van Liefde.

Bovenop deze wettelijke vereisten vinden wij het ook vanuit ethisch standpunt onze opdracht om de persoonlijke levenssfeer van de cliënten en de medewerkers te respecteren. We streven daarin zorgvuldigheid na en overleg met de betrokkenen. We hechten ook groot belang aan het respecteren van het beroepsgeheim en de discretie.

3.3 Een lerende organisatie

We zijn er ons van bewust dat informatiebeveiliging net als veiligheid op andere terreinen niet voor 100% haalbaar is. Daaruit leiden we af dat verbeteringen altijd mogelijk zijn en dat we dus blijvend kunnen bijleren. We beschouwen onszelf daarom als een lerende organisatie die bij incidenten de mogelijke oorzaken analyseert en preventiemaatregelen uitwerkt en niet in de eerste plaats een ‘dader’ zoekt. Een lerende organisatie betekent ook medewerkers sensibiliseren voor risico’s en zorgvuldig gedrag promoten. We willen ook op vlak van informatiebeveiliging een leer- en verbetercultuur bevorderen.

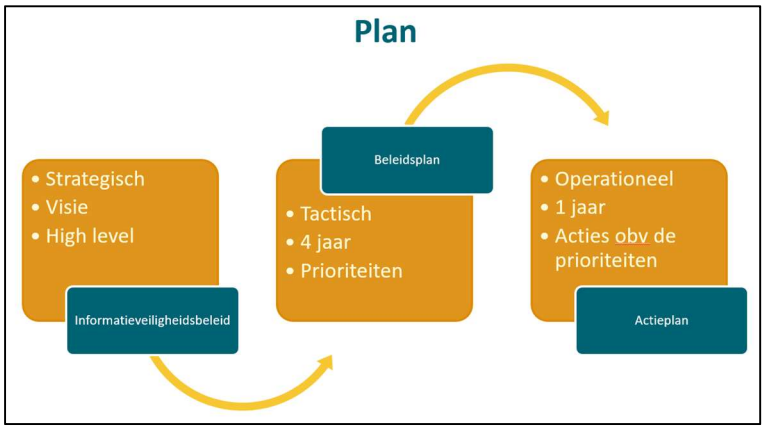
3.4 Realisme

Dit informatiebeveiligingsbeleid gaat voor een realistische aanpak. Daar zijn twee aspecten aan. Ten eerste zonder inzet van middelen (human resources en geld) kunnen we geen beleid voeren dat informatiesystemen passend beveiligt. Ten tweede kunnen maatregelen op vlak van informatiebeveiliging soms financiële kosten impliceren of een impact hebben op de tijd die medewerkers aan hun kernopdracht kunnen besteden. De middelen zijn niet onbeperkt en een afweging van de kosten in geld en tijd is nodig.

We gaan dus voor een zo hoog mogelijk beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van persoons- en bedrijfsgegevens en voor een efficiënt gebruik van de beschikbare middelen.

4 Het managementsysteem voor informatiebeveiliging

Om het informatiebeveiligingsbeleid kwaliteitsvol en actueel te houden zal het door middel van de Plan-Do-Check-Act cyclus worden beoordeeld en bijgestuurd via het operationeel beleid. Het strategisch beleid vormt de basis waarop het operationeel beleid gebaseerd is en wordt om de vier jaar herwerkt of indien het noodzakelijk is. Jaarlijks worden alle beheersmaatregelen overlopen in het licht van de actuele risico's en het opstellen van het jaaractieplan. Het jaaractieplan wordt op elke Centrale Stuurgroep Gegevensbescherming besproken en eventueel bijgestuurd.

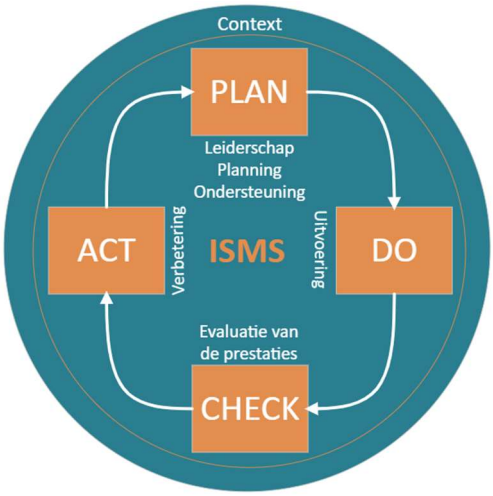


4.1 Bewustwording en training

Een beleid is maar zo krachtig als het gekend en toegepast wordt binnen de Groep Broeders van Liefde. Vanuit de DPO-office[11] zullen afspraken, richtlijnen, adviezen en tips ter beschikking worden gesteld om de bewustwording bij de medewerkers te verhogen. Er zal jaarlijks een bewustwordingsplan uitgewerkt worden met concrete invulling waarmee snel aan de slag kan worden gegaan.

4.2 Managementsysteem informatiebeveiliging

Om onze doelstellingen op het vlak van gegevensbescherming (informatiebeveiliging) te halen, wordt gebruik gemaakt van de ISO 27K (overeenkomstig de Maturiteitsmeting en NIS-2), toegepast op PDCA-cyclus.



[11] Zie '5 Rollen en verantwoordelijkheden'.

Plan

- *Hoofdstuk 5 Leiderschap*[12]
  - *Leiderschap en betrokkenheid*
  - *Informatiebeveiligingsbeleid*
  - *Rollen, verantwoordelijkheden en bevoegdheden*
- *Hoofdstuk 6 Planning*
  - *Risico's beperken en kansen benutten*
  - *Informatiebeveiligingsdoelstellingen*
  - *Planning van wijzigingen*
- *Hoofdstuk 7 Ondersteuning*
  - *Middelen voor het managementsysteem*
  - *Competentie*
  - *Bewustzijn*
  - *Communicatie*
  - *Gedocumenteerde informatie*

Do

- *Hoofdstuk 8 Uitvoering*
  - *Operationele planning & beheersing*
  - *Risicobeoordeling uitvoeren*
  - *Risicobehandeling uitvoeren*

Check

- *Hoofdstuk 9 Evaluatie van de prestaties*
  - *Monitoren, meten, analyseren en evalueren*
  - *Interne audit*
  - *Management review*

Act

- *Hoofdstuk 10 Verbetering*
  - *Continue verbetering*
  - *Afwijkingen en corrigerende maatregelen*

In het operationeel beleidsplan worden de risico's ingeschat op basis van de beheersmaatregel. Het doel is om voor elke beheersmaatregel een zo hoog mogelijk maturiteitsniveau te halen. Deze maatregelen worden gekoppeld aan, verbonden met, de CyberFundamentals. Het plan van aanpak wordt uitgeschreven in jaardoelstellingen.

4.3 Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is een strategisch document dat verder wordt uitgewerkt in verschillende beleidsdocumenten, afspraken en richtlijnen. Deze beveiligingsmaatregelen en andere relevante documenten in relatie tot dit informatiebeveiligingsbeleid zijn te raadplegen op de SharePoint.

Volgende niet limitatieve lijst van documenten wordt uitgewerkt en ter beschikking gesteld van de medewerkers.

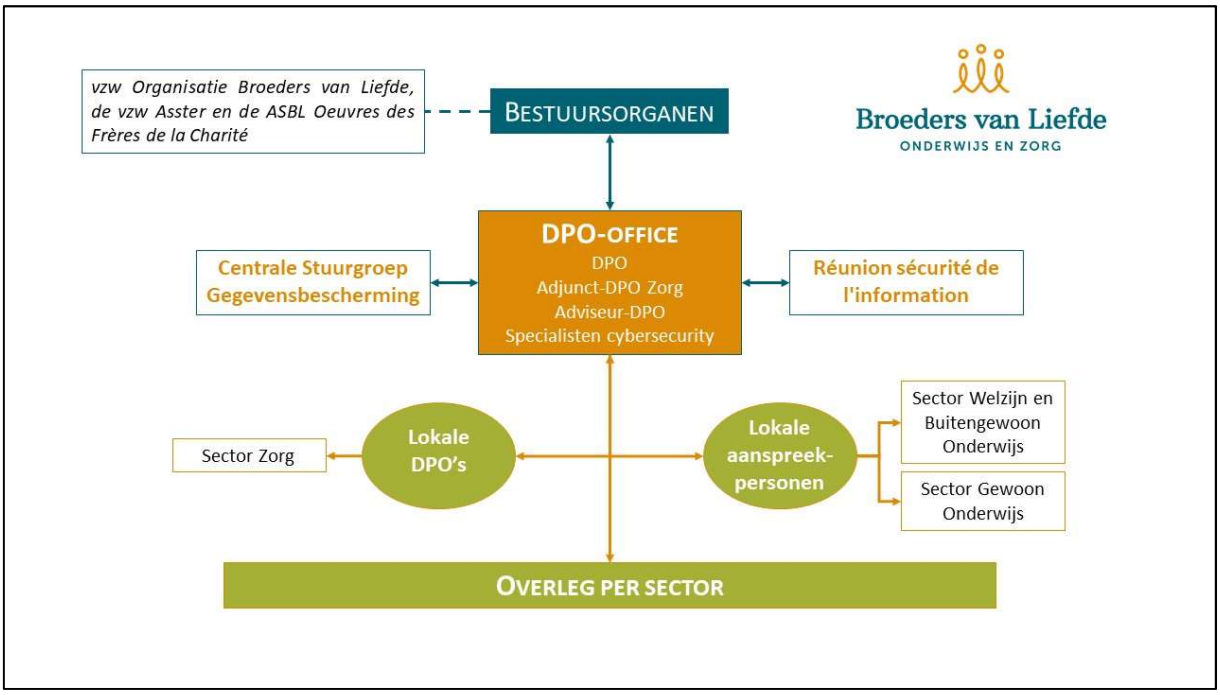
- Incidentresponsplan;
- Uitleg van begrippen (bijvoorbeeld persoonsgegevens, datalekken, doorgiftemechanisme);
- Een omschrijving van de (categorieën van) persoonsgegevens;
- Een beschrijving van de rechten van betrokkenen;
- Toezicht en handhaving;
- De rol van de (lokale) DPO / aanspreekpersoon
- ...

[12] De structuur is overgenomen uit de ISO 27001-2022. De titels van de eerste vier hoofdstukken zijn: '*Hoofdstuk 1 Introductie*', '*Hoofdstuk 2 Referenties*', '*Hoofdstuk 3 Termen en Definities*', '*Hoofdstuk 4 Context van de Organisatie*', '*Hoofdstuk 5 Leiderschap*', […].

4.4 Monitoring en evaluatie

Op de eerste Centrale stuurgroep Gegevensbescherming van elk jaar wordt steeds tijd voorzien voor de evaluatie en herziening van het informatiebeveiligingsbeleid in het licht van veranderende bedreigingen en technologieën. Om het beleid adequaat te kunnen opvolgen en bijsturen zal gebruik gemaakt worden van de PDCA-cyclus. Anderzijds zullen interne en externe audits uitgevoerd worden.

5 Rollen en verantwoordelijkheden



5.1 Medewerkers van de Groep Broeders van Liefde

Alertheid en bewust omgaan met data en informatie is de basiscompetentie van elke medewerker. Het is ieders verantwoordelijkheid om die situaties te identificeren waar risico's aan verbonden zijn m.b.t. informatiebeveiliging. Door kennis te nemen van het informatiebeveiligingsbeleid en de bijhorende afspraken en richtlijnen toe te passen staan we sterker tegen bedreigingen. Door incidenten te melden kunnen we samen datalekken voorkomen, maar ook leren uit de situatie en kunnen we de processen bijsturen waar mogelijk. Een hoeksteen is het aanbieden van vormingen, sensibilisering, intervisie, … m.b.t. informatiebeveiliging en privacy.

5.2 Bestuursorganen

De Bestuursorganen zijn de eindverantwoordelijke op het vlak van het informatiebeveiligingsbeleid. Via de verschillende overlegstructuren wordt het beleid uitgedragen en vormgegeven. Het bestuursorgaan stelt de nodige middelen (financieel, human resources en materiaal) ter beschikking om een gedegen informatiebeveiligingsbeleid binnen de organisatie te kunnen voeren.

5.3 Lokale directie

Het is de verantwoordelijkheid van de lokale directie om het beleid, op advies van de DPO, te implementeren.

5.4 Centrale Stuurgroep Gegevensbescherming

De Centrale Stuurgroep Gegevensbescherming maakt de voorbereidingen en coördinatie van het beleidsplan. De CSGGB legt de relevante adviezen ter bekrachtiging voor aan de bestuursorganen. Het beleid wordt ook besproken op de Réunion de Securité de l'Information et GDPR.

5.5 Functionaris voor gegevensbescherming[13]

De centrale aanspreekpersoon neemt de rol van 'functionaris voor gegevensbescherming' op, zoals beschreven in artikelen 37 t/m 39 van de GDPR, voor de Groep Broeders van Liefde. De DPO is verantwoordelijk voor de uit- en bijwerking van het beleid en laat zich hierin bijstaan door de Adjunct-DPO zorg. Op de Centrale Stuurgroep Gegevensbescherming en de Réunion de Securité de l'Information et GDPR worden het beleid en de bijhorende afspraken en richtlijnen besproken en goedgekeurd. De DPO is onder meer het aanspreekpunt voor cliënten, medewerkers en leveranciers die meer informatie willen over de bescherming van hun gegevens of over hun rechten, of die een klacht willen indienen. De DPO is het contactpunt voor o.a. de Belgische Gegevensbeschermingsautoriteit (GBA), eHealth en de Vlaamse Toezichtscommissie (VTC). De DPO werkt samen met de Adjunct-DPO zorg en vormen samen de DPO-office. Zij vragen advies aan o.a. collega's werkzaam op de IT-diensten (lokaal en centraal) en de juridische dienst, om een goed en gedragen informatiebeveiligingsbeleid met bijhorende richtlijnen en afspraken te kunnen uitschrijven.

5.6 Lokale DPO's/aanspreekpersonen

Binnen elke voorziening (ziekenhuis, school, woonzorgcentrum…) is een lokaal aanspreekpersoon aangesteld. Binnen de sector Zorg wordt per zorggroep een lokale DPO aangesteld. De sector Gewoon Onderwijs (GO) en de sector Welzijn en Buitengewoon Onderwijs (WBuO) voorzien minimaal één aanspreekpersoon per cluster. Binnen de sector GO en WBuO mag ook gekozen worden om per cluster te werken of per voorziening of per campus. Het is aan de lokale DPO's/aanspreekpersonen om het beleid te bespreken met de lokale directie en te implementeren. Elke aanspreekpersoon zorgt dat er binnen zijn voorziening van tewerkstelling op regelmatige tijdstippen een overlegmoment is ingepland met de directie en het hoofd van de IT-dienst. De lokale aanspreekpersonen zullen jaarlijks meerdere malen samenkomen voor onderling overleg met de centrale DPO en adjunct DPO Zorg.

5.7 Team ICT

Lokale en centrale ICT-teams zorgen voor de technische implementatie van de beveiliging van elektronische gegevens en van de systemen die deze gegevens ter beschikking stellen. Zij vertalen de aanbevelingen of vereisten van het beleid in concrete maatregelen op systemen, netwerken, databanken, toestellen en applicaties.

[13] In het Nederlands spreken we over de '*Functionaris voor gegevensbescherming*', in het Frans over '*Délégué à la protection des données*', en in het Engels '*Data Protection Officer*', en afgekort als 'DPO'.