Beleidsnotitie:	Privacybeleid	
Publicatiedatum:	Oktober 2022	
Beoordelingscyclus:	3e kwartaal 2025	

INHOUDSOPGAVE

1 INLEIDING

1.1 Aanleiding

SGL biedt ondersteuning en begeleiding op maat aan mensen met een niet-aangeboren hersenafwijking om binnen de eigen mogelijkheden het leven te leiden dat ze zelf willen. Daarbij zet SGL behandelaars, begeleiders, vervoerders en vrijwilligers in. Een groot deel van deze mensen werkt met bijzondere persoonsgegevens van cliënten van SGL.

SGL onderkent dat het voor haar professionele dienstverlening essentieel is dat deze persoonsgegevens goed beschermd zijn en dat de bescherming in overeenstemming moet zijn met vigerende wet- en regelgeving. De Algemene Verordening Gegevensbescherming (AVG) is hier een voorbeeld van.

1.2 Toelichting

Iedere organisatie binnen de EU die een service, product of dienst aanbiedt, dient te voldoen aan de Europese privacywetgeving: de Algemene Verordening Gegevensbescherming (AVG). De AVG is vanaf 25 mei 2018 van kracht en vervangt vanaf dat moment binnen Nederland de tot dan geldende Wet bescherming persoonsgegevens (WBP). De AVG beschermt kort gezegd de privacybelangen van personen binnen Nederland en de EU.

1.3 Doelstelling

Het verwerken van persoonsgegevens is onmisbaar bij het invullen van taken die voortvloeien uit de dienstverlening door SGL. Het is zaak dat de cliënten maar ook medewerkers, uitzendkrachten, vrijwilligers etc ten alle tijden een veilig gevoel hebben als zij informatie delen met SGL. Duidelijke communicatie over hoe SGL met de gegevens van deze betrokkenen omgaat is in deze hoedanigheid belangrijk voor de continuïteit van de informatiestroom.

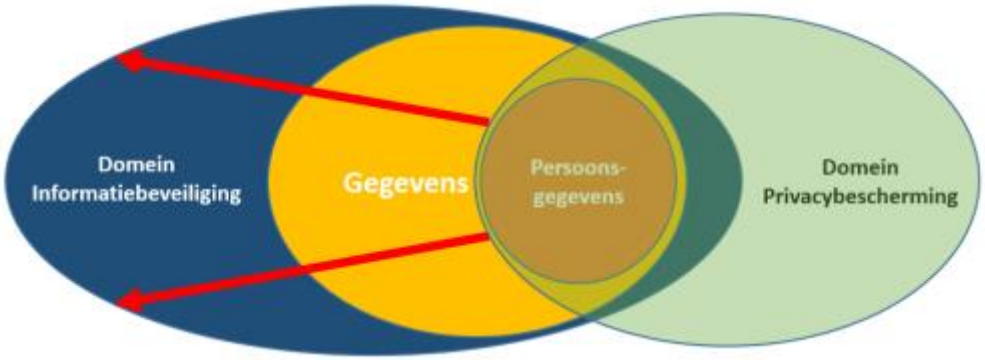
Het privacybeleid geeft aan op welke wijze - door het treffen van maatregelen – voldaan wordt aan de van toepassing zijnde wet- en regelgeving.

1.4 Juridisch kader

De AVG regelt het algemene kader voor de omgang met privacy in ons land. De AVG is te beschouwen als parapluwetgeving die van toepassing is op bijna alle sectoren, instellingen en bedrijven in de EU. Voor het verwerken van persoonsgegevens voor privégebruik geldt de AVG niet. De AVG vereist dat voor welke verwerking van persoonsgegevens een beroep kan worden gedaan op één van de in artikel 8 AVG genoemde grondslagen. Na vaststelling van die grondslag is het vervolgens mogelijk om op gestructureerde wijze te bepalen welke verwerking, van welke persoons-gegevens, voor welke doeleinden rechtmatig en noodzakelijk is. Daarnaast zijn in tal van bijzondere wetten regels met betrekking tot privacy opgenomen. In bijlage A wordt een opsomming gegeven van relevante regelgeving.

1.5 Samenhang tussen informatiebeveiliging en privacybescherming

Informatiebeveiliging omvat het geheel aan maatregelen waarmee organisaties hun informatie (gegevens), maar ook processen beveiligen. Deze maatregelen zijn gericht op het waarborgen van de betrouwbaarheid, bestaande uit integriteit, continuïteit en vertrouwelijkheid.
De *privacywetgeving* richt zich specifiek op *persoonsgegevens*, waarbij de eis tot beveiligen (passende technische en organisatorische maatregelen) overeenkomt met de doelstelling van informatiebeveiliging. Daarnaast stelt de privacywet eisen aan het gebruik (verkrijgen, verwerken, bewaren, etc.) van de persoonsgegevens. Genoemde relatie is onderstaand visueel weergegeven.



1.6 Samenhang tussen privacybescherming en risicomanagement

Oplossingen kosten doorgaans geld, direct of indirect. De wet staat toe dat er een redelijke afweging gemaakt wordt tussen doel en kosten.
Om te bepalen of een investering opweegt tegen de baten dient er duidelijkheid te zijn over de privacy risico's (en imagoschade risico's) die ermee afgedekt of verminderd worden.
Te dure of complexe maatregelen leiden tot een onevenredig zware last en maken de dienstverlening duur; dat is niet in het belang van de betrokkene en niet in het belang van de organisatie.

1.7 Werkingsgebied

Het werkingsgebied van het privacybeleid van SGL strekt zich uit tot de verantwoordelijkheden voor informatiebeveiliging van interne belanghebbenden (de bedrijfsgegevens van SGL zelf en externe belanghebbenden (cliënten, relaties, leveranciers).

1.8 Belanghebbenden

Binnen SGL kunnen de volgende belanghebbenden onderscheiden worden:

1. Cliënten/wettelijke vertegenwoordigers: persoonsgegevens die SGL verwerkt van cliënten

2. Contactpersonen organisaties: het gaat hierbij om de contactgegevens van contactpersonen bij de organisaties waarmee SGL samenwerkt.
3. Vrijwilligers
4. Medewerkers: medewerkers van SGL als ook tijdelijke of externe arbeidskrachten die SGL inhuurt en waarvan persoonsgegevens worden verwerkt.

De medewerkers zijn aan de hand van de voortgangsstadia ingedeeld in de volgende categorieën:
- Sollicitanten
- Werknemers
- Ex-werknemers

1.9 Verantwoordelijkheid voor privacybeleid

Organisaties die persoonsgegevens verwerken zijn verantwoordelijk dit op de juiste wijze binnen de wettelijke kaders te doen. In de AVG wordt de term "verantwoordelijke" veelvuldig gebruikt. De verantwoordelijke is diegene op wiens gezag persoonsgegevens worden verwerkt en die, in deze hoedanigheid, dus ook het doel van de verwerking bepaalt.
Binnen SGL bepaalt de Raad van Bestuur het beleid, de strategie en de koers van de organisatie. In die hoedanigheid wordt de Raad van Bestuur dan ook gekenmerkt door de wetgever als "de verantwoordelijke".
Het is de taak van de Raad van Bestuur om een privacy strategie te formuleren die op tactisch en strategisch niveau door de gehele organisatie gedragen wordt.

1.10 Communicatie van het privacybeleid

Privacy is voor een belangrijk deel een zaak van bewustwording, cultuur en communicatie. Bestuur, medewerkers en andere belanghebbenden moeten zich voortdurend bewust zijn van het belang van het waarborgen van de rechten van de cliënten.
Naast het inrichten van het privacybeleid en werkprocessen is het van belang dat de personen die daadwerkelijk werken met deze gegevens weten wat hun verantwoordelijkheid is en hoe ze zorgvuldig om moeten gaan met persoonsgegevens. Daarom is het belangrijk dat de medewerkers zich bewust zijn van de regels en gedragsnormen rondom privacy.
SGL zal dit proces ondersteunen door het ontwikkelen van bijvoorbeeld privacy protocollen en afwegingskaders. Richting cliënten is communicatie over de privacy van belang. De client heeft het recht te weten wat er met zijn of haar gegevens gebeurt. De medewerkers moeten zich bewust zijn van het belang van privacy en hoe zij persoonsgegevens op een zorgvuldige manier dienen te verwerken. Er worden trainingen georganiseerd over hoe zij met privacyvraagstukken om moeten gaan in hun functie en/of rol.

Dit zal gebeuren in de vorm van een voor iedereen verplichte e-learning Informatiebeveiliging en Privacy. SGL streeft een cultuur na waarbij medewerkers elkaar in alle openheid aanspreken op het eigen gedrag rondom privacy en daarmee van elkaar leren. Communicatie, openheid en toetsing zijn belangrijke randvoorwaarden voor het realiseren van een optimaal privacybeleid.

2 VERANTWOORDINGSPLICHT AVG

2.1 Algemeen

SGL heeft volgens de AVG tot taak om persoonsgegevens zo goed mogelijk te beschermen en dit aantoonbaar te maken. Hiervoor zijn de volgende *verplichte* maatregelen van toepassing:

1. Het bijhouden van een verwerkingsregister: dit is een overzicht van de verwerkingen van persoonsgegevens die binnen een organisatie plaatsvinden;
2. Het uitvoeren van een *data protection impact assessment* (DPIA): hiermee worden de privacy risico's bij de verwerking van persoonsgegevens met een hoog privacy risico in kaart gebracht. Hiermee kan aangetoond worden waarom de beoogde verwerking noodzakelijk is en worden de getroffen maatregelen om de risico's aan te pakken weergegeven;
3. Het bijhouden van een register van datalekken: hierin worden de inbreuken in verband met persoonsgegevens opgenomen. In dit register staan zowel de datalekken die gemeld moeten worden bij de toezichthouder als die waarvoor geen meldplicht geldt;
4. Aantoonbaar toestemming verkrijgen: voor de verwerking van persoonsgegevens is toestemming vereist. SGL moet kunnen aantonen dat er daadwerkelijk toestemming van de betrokkene is verkregen. De betrokkene moet deze toestemming vrijelijk, ondubbelzinnig , geïnformeerd en specifiek hebben gegeven;
5. De verplichte aanstelling van een Functionaris Gegevensbescherming (FG): aangezien SGL op grote schaal bijzondere persoonsgegevens (medische gegevens) verwerkt, dient er verplicht een FG aangesteld te zijn.

2.2 Rechtmatigheid

De verwerking van persoonsgegevens is rechtmatig als tenminste aan één van de volgende voorwaarden is voldaan:

1. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
2. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de Zorg- en dienstverleningsovereenkomst);
3. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting (bijvoorbeeld de uitvoering van de WMO);
4. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen (bijvoorbeeld wanneer er acuut gevaar dreigt maar iemand is bewusteloos of mentaal niet in staat om toestemming te verlenen);
5. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag (bijvoorbeeld een gemeente die cameratoezicht inzet voor de openbare orde);
6. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van SGL en deze belangen zwaarder wegen dan de belangen van de betrokkene (bijvoorbeeld SGL dient ook haar zorgplicht voor haar werknemers na te komen).

2.3 Transparantie

Er zijn een aantal vereisten waar de verstrekking van informatie aan en de communicatie met betrokkenen moet voldoen:

- De informatie of communicatie moet beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk zijn;
- Er moet duidelijke en eenvoudige taal gebruikt worden;
- De informatie moet schriftelijk of met andere middelen, met inbegrip van indien dit passend is, elektronische middelen worden verstrekt;
- De informatie moet over het algemeen kosteloos worden verstrekt.

2.4 Doelbinding

Doelbinding is essentieel binnen de AVG en houdt in dat persoonsgegevens alleen verzameld en gebruikt mogen worden voor een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel. Zo dienen bijvoorbeeld sollicitatiegegevens vernietigd te worden, zodra een sollicitant niet aangenomen wordt. Het doel beperkt ook de mogelijkheid om persoonsgegevens die eenmaal voor een bepaald doel verzameld zijn voor een ander doel te gebruiken.

2.5 Juistheid

De nauwkeurigheid van persoonlijke gegevens vormt een integraal onderdeel van gegevensverwerking. De AVG stelt dat "alle redelijke maatregelen moeten worden genomen" om gegevens die onjuist of onvolledig zijn te wissen of te rectificeren.

2.6 Beveiliging van de verwerking

Wettelijke basis
Volgens artikel 32, lid 1 van de AVG dient SGL 'passende technische en organisatorische maatregelen' te treffen om het verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen. Onder 'passend' wordt hier verstaan de afstemming van de *zwaarte* van de beveiligingsmaatregelen op basis van het *risico* van de verwerking. Door een risicoanalyse of 'Data Protection Impact Assessment' (DPIA) uit te voeren worden de risico's inzichtelijk. Vervolgens wordt op basis van de resultaten een keuze gemaakt.

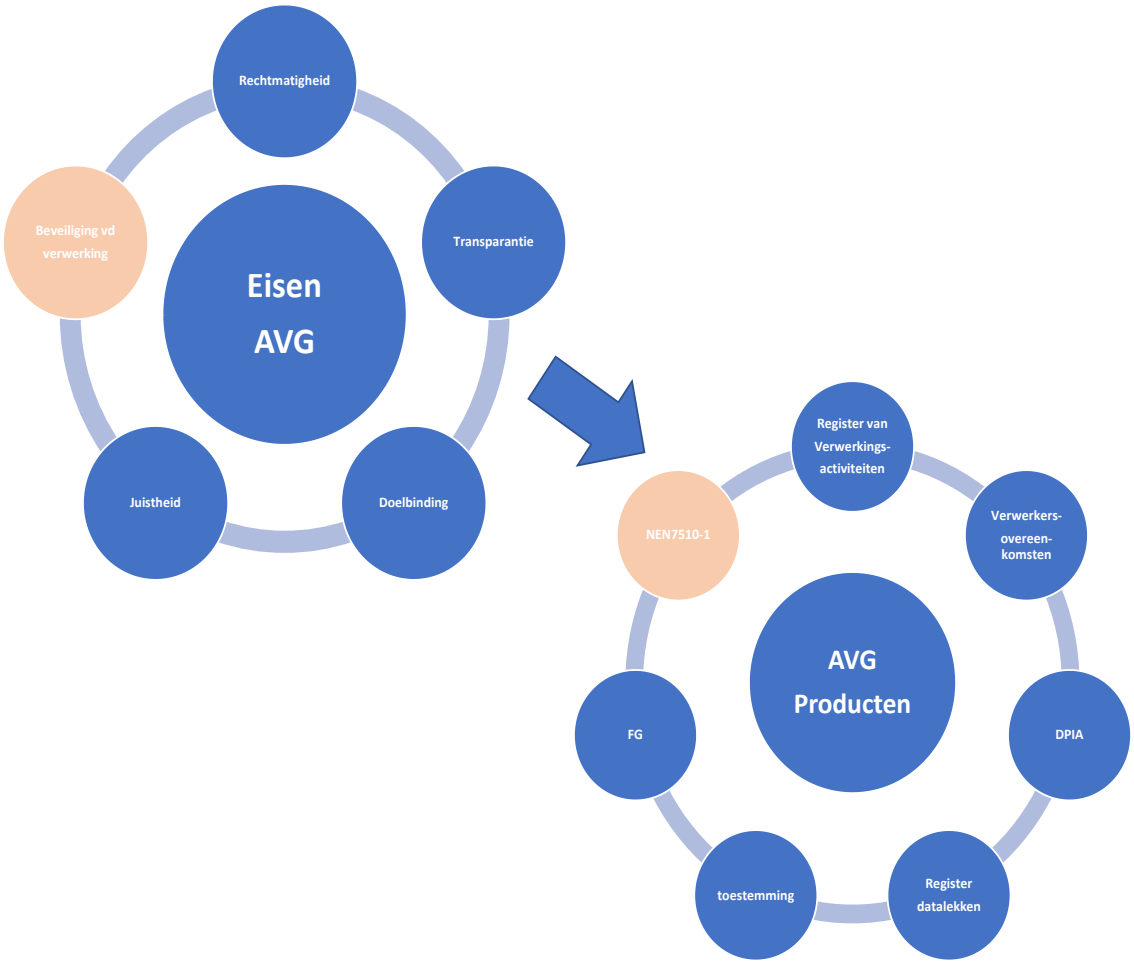
Technische maatregelen
Dit kunnen zowel fysiek als digitale technische voorzieningen zijn. Deze zijn onder andere gericht om verlies en/of onrechtmatige verwerkingen en inbreuken op de beveiliging van persoonsgegevens te voorkomen of te beperken.
Voorbeelden (*niet uitputtend*) hiervan zijn:

- Fysieke toegangsbeveiliging;
- Toepassen van encryptie;
- Hanteren van een wachtwoordbeleid;
- Tweefactor authenticatie (MFA);
- Periodiek back-ups maken van systemen;
- Een firewall gebruiken;
- Virus- en malwarescanners;
- Het bijhouden van logfiles;

Organisatorische maatregelen
Hierbij worden maatregelen bedoeld die de toegang tot persoonsgegevens beperken waardoor alleen bevoegde personen toegang krijgen.
Voorbeelden (niet uitputtend) hiervan zijn:

- Het loggen (registreren) van wie toegang heeft gehad tot gegevens;
- Het periodiek houden van interne audits;
- Clean desk en clear-screen beleid;
- Het opstellen en afsluiten van verwerkersovereenkomsten;
- De verplichtstelling tot het deelnemen aan een e-learning in het kader van de bevordering van AVG awareness.

Toepassing SGL
In de lijn met het gestelde in art. 32, lid 3[1] zal SGL voldoen aan het gestelde in art. 32, lid 1, *door compliant te zijn met de NEN7510 norm voor informatiebeveiliging voor de zorg.*
Een separaat informatiebeveiligingsbeleid is hiertoe (o.a.) vastgesteld.



Figuur 1: Grafische voorstelling Relatie Verantwoordingsplicht AVG en producten

[1] art. 32, lid 3 geeft de mogelijkheid om te voldoen aan art. 32, lid 1 door aansluiting bij een gedragscode of goedgekeurd certificeringsmechanisme conform art. 42.

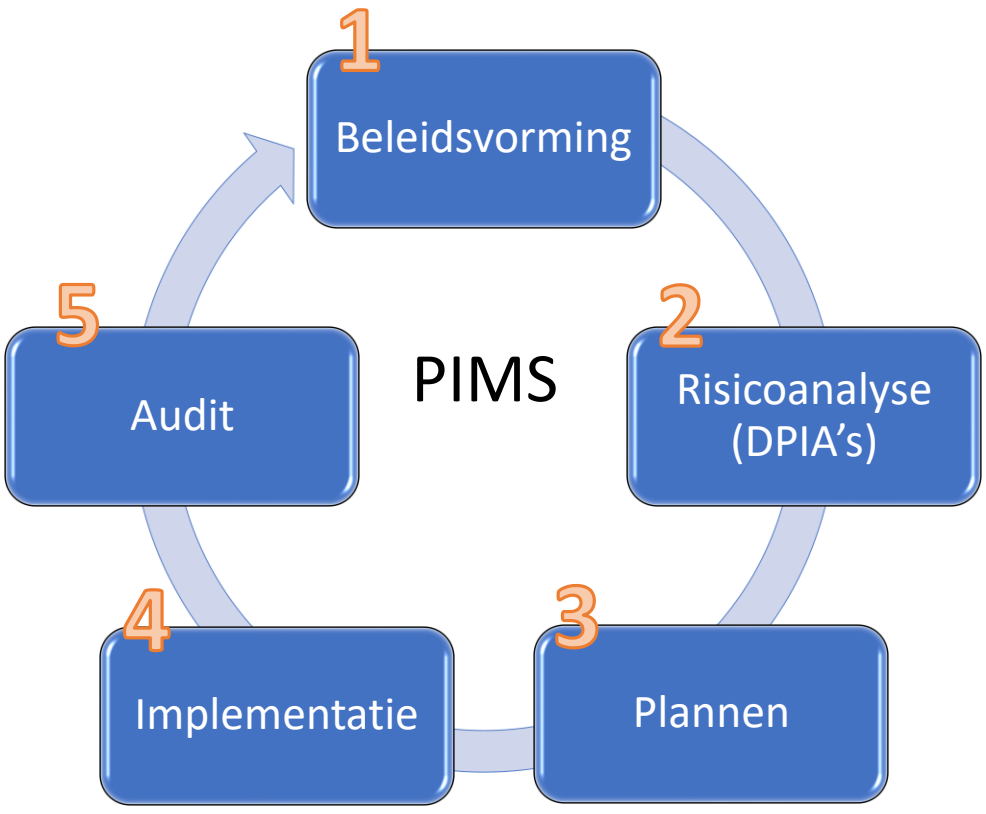
3 MANAGEMENTSYSTEEM VOOR PRIVACYBESCHERMING VOOR SGL (PIMS)[2]

3.1 Algemeen

Alle stakeholders van SGL moeten erop kunnen vertrouwen dat hun gegevens in veilige handen zijn. Daarom is niet alleen op het gebied van informatiebeveiliging maar ook op het gebied van privacybescherming een managementsysteem ingericht dat gebaseerd is op de NEN7510 norm en de AVG.
Dit managementsysteem voorziet in een continu proces van verbeteren en borgen van de kwaliteit op basis van *Plan-Do-Check-Act* (PDCA) cyclus[3].

3.2 Cyclisch proces

Een vijftal fasen vormen tezamen een continue cyclus, de eerder genoemde PDCA-cyclus (zie onderstaande figuur) Deze cyclus zorgt er voor dat het privacybeleid de laatste stand van zaken op het gebied van norm-, wetgeving en technische beveiligingsmaatregelen volgt.



Figuur 2: Privacy Information Management System

[2] De basis voor het hier genoemde managementsysteem is de NEN-ISO/IEC 27701:2019 'Uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacy-informatiemanagement – Eisen en richtlijnen'
[3] Plan-Do-Check-Act cyclus van Deming

3.2.1 Beleidsvorming

Het managementsysteem voor privacybescherming start met het opstellen van het privacybeleid (*voorliggend document*). In dit beleid worden de doelstellingen en uitgangspunten voor privacybescherming van SGL vastgelegd.

De Raad van Bestuur van SGL stelt het beleid vast.

Hiermee vormt het beleid de leidraad voor de overige stappen van het managementsysteem.

3.2.2 Risicoanalyse

De AVG verwacht van organisaties dat zij bewust omgaan met privacy, hiervoor moeten de risico's in kaart gebracht worden. Vervolgens dienen deze risico's geanalyseerd te worden: als de gebeurtenis zich voltrekt, wat voor gevolg brengt dat dan met zich mee ? En hoe groot is de kans dat het risico zich voordoet ?

Hiertoe zullen binnen SGL gegevenseffectbeoordelingen (DPIA[4]'s) uitgevoerd worden door de medewerker Informatiebeveiliging en Privacy, indien nodig, in overleg met de desbetreffende eigenaar van het systeem. Over DPIA's zal een advies worden uitgebracht door de Functionaris gegevensbescherming.

3.2.3 Planvorming

In deze fase worden de informatiedoelstellingen en de relevante processen en procedures gedefinieerd. Hierbij wordt niet alleen het algemeen privacybeleid beschreven maar ook de onderliggende beleidsdocumenten en regelingen.

3.2.4 Implementatie

Gedurende deze fase worden het beleid en de onderliggende documenten geïmplementeerd en de verantwoordelijkheden belegd.

3.2.5 Monitoring/evaluatie/controle

Op basis van zelfcontrole (een interne of externe audit) worden indien nodig maatregelen genomen om er voor te zorgen dat het privacybeleid wordt nageleefd. Indien de uitkomsten van de audit hiertoe aanleiding geven kan het beleid worden aangescherpt/aangepast.

[4] In de GDPR (basis voor AVG) genoemd 'Data Protection Impact Assessment'

3.3 Inpassing in de bedrijfsvoering van SGL

3.3.1 Organisatie/rollen/verantwoordelijkheden

Binnen SGL worden privacy-kritische taken toegekend aan de volgende functies/rollen:

Functionaris Gegevensbescherming:

- Centrale aanspreekpunt voor privacy gerelateerde zaken binnen SGL;
- Controlerende rol m.b.t. de volgende zaken:
  - Gevraagd en ongevraagd *onafhankelijk* informeren en adviseren van RvB over haar verplichtingen inzake de eisen die de AVG stelt aan rechtmatige gegevensverwerking;
  - Controleren en bewaken van het privacy awareness niveau;
  - Toezien op het naleven van de eisen die de AVG stelt aan rechtmatige gegevensverwerking;
  - Toewijzing van verantwoordelijkheden en taakverdeling;
  - Advies verstrekken m.b.t. de gegevenseffectbeoordelingen (DPIA);
  - Samenwerking met de toezichthoudende autoriteit AP.

Medewerker Informatiebeveiliging en Privacy

- Interne regelingen, procedures en programma's ontwikkelen ten behoeve van rechtmatig werken;
- Implementeren en afstemmen van technische en organisatorische maatregelen;
- Inventarisatie van de gegevensverwerking en bijhouden middels het verwerkingsregister;
- Opstellen en bijhouden van de privacyverklaring en toestemmingsprocedures (transparantie);
- Planning en controle privacy verbeterplan (korte, middel- en lange termijn);
- Controleren, opstellen en afsluiten van contracten (verwerkers-overeenkomsten);
- Afhandelen van privacy vraagstukken;
- Input leveren bij het opstellen of aanpassen van de gedragscode;
- Bevorderen van privacy-awareness bij medewerkers;
- Inrichten en uitvoeren van proces meldplicht datalekken;
- Adviseren over technologie en beveiliging (privacy-by-design);
- Uitvoeren van DPIA's.

Adviesgroep Informatiebeveiliging en Privacy (AIP)

- Binnen SGL is, conform NEN7510-1:2020, een zogenaamd 'informatiebeveiligings-managementforum' (IBMF) actief. Dit IBMF wordt binnen SGL aangeduid met "Adviesgroep Informatiebeveiliging & Privacy" oftewel AIP. De AIP heeft, naast informatiebeveiliging dus óók privacybescherming als aandachtsveld, beiden zijn immers sterk aan elkaar verbonden.

De AIP heeft voor AVG-gerelateerde vraagstukken een belangrijke rol als klankbord en *adviesorgaan* naar RvB/MT. De AIP wordt voorgezeten door de medewerker Informatiebeveiliging en Privacy.

3.3.2 Auditering/controle

Eenmaal per jaar wordt binnen SGL in het kader van de PDCA cyclus de effectiviteit van het privacybeleid en maatregelen getoetst.
Dit wordt gedaan middels een audit (intern of extern), waarvan de reikwijdte wordt vastgesteld in een auditplan.
Deze audit maakt onderdeel uit van de interne kwaliteitscyclus.

3.3.3 Rapportage en frequentie

De PDCA-cyclus vereist regelmatige rapportage over de status en voortgang van de privacyveiligheid binnen SGL.

- Jaarlijks wordt het privacybeleid op onderdelen geauditeerd op initiatief van het RvB (zie 3.3.2). Dit kan de vorm van een interne òf externe controle aannemen.
- Eenmaal per jaar wordt het privacyplan herzien op initiatief van de AIP en voorgelegd aan RvB/management.
- Minstens eenmaal per 3 jaar wordt het privacybeleid herzien op initiatief van de AIP en vastgesteld door RvB.

3.3.4 Onafhankelijke beoordeling

- Eenmaal per jaar wordt over de status van informatieveiligheid & privacy binnen SGL *onafhankelijk* gerapporteerd aan het RvB/management-overleg door de FG.

- De FG geeft gevraagd én ongevraagd adviezen over AVG-gerelateerde kwesties en rapporteert hierover *direct aan RvB*. RvB oordeelt als Verwerkingsverantwoordelijke of deze adviezen worden overgenomen en geeft hieromtrent zo nodig instructies aan de lijnverantwoordelijke(n).

BIJLAGE A: RELEVANTE WETGEVING

SGL streeft er naar te voldoen aan alle van toepassing zijnde wet- en regelgeving:

- Wet langdurige zorg (Wlz);
- Wet maatschappelijke ondersteuning (Wmo);
- Wet Geneeskundige Behandelingsovereenkomst (WGBO);
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz);
- Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG);
- Wet Zorg en Dwang (WZD);
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz);
- Algemene Verordening Gegevensbescherming/Uitvoeringswet AVG (UAVG).
- Wet Meldplicht Datalekken (WMD)

BIJLAGE B: BEWAARTERMIJNEN

Cliëntgegevens (medisch en zorg)

Samenvatting: De wet schrijft een bewaartermijn van cliëntdossiers voor van **20 jaar** (**twintig)** na afloop van de behandeling.

Persoonsgegevens medewerkers

De Belastingdienst schrijft voor dat fiscale gegevens (onder andere loonbelastingverklaring en kopie ID) **tenminste vijf jaar** worden bewaard. Voor andere personeelsgegevens geldt een bewaartermijn van **maximaal twee jaar.** In onderstaande tabel een opsomming van data en bewaartermijnen volgens best practice (sommige waarvan al bij SGL in gebruik):

Soort gegevens	**Bewaartermijn en relevante wetgeving**
Gegevens die **fiscaal relevant** zijn	**7 jaar** Algemene Wet inzake Rijksbelastingen (AWR)
Gegevens betreffende **etniciteit en herkomst** van medewerkers	**5 jaar** Wet stimulering Arbeidsdeelname Minderheden – Wet Samen
Overige gegevens van medewerkers (actieve registratie)	Uiterlijk tot **2 jaar** na uitdiensttreding
Personeelsdossiers (archief)	**10 jaar**
Voor verschillende **HR-gegevens** geldt een bewaarplicht van zeven jaar, ook als een werknemer niet meer in dienst is. Het gaat om: persoonlijke gegevens zoals naam, adres, woonplaats, burgerlijke staat datum indiensttreding salarisadministratie arbeidsvoorwaarden (aanvullende arbeidsafspraken, salarisafspraken) afstandsverklaring woon-werkverkeer afspraken in verband met levensloopregeling samenleving/partnerschap	**7 jaar**
Voor enkele andere **HR-gegevens** geldt een bewaartermijn van één jaar: sollicitatiegegevens (brief, formulier, CV, referenties, getuigschrift) gegevens uit psychologisch onderzoek	**Zonder toestemming 4 weken, met toestemming maximaal 1 jaar**

Soort gegevens	**Bewaartermijn en relevante wetgeving**
De volgende **papieren** moet u tot vijf naar na het einde van het dienstverband bewaren en dient u daarna te vernietigen: loonbelastingverklaringen (ook de loonbelastingverklaringen die zijn vervangen door nieuwe) kopie van identiteitsbewijs	**5 jaar**
Overig	
concurrentiebeding:	Zolang het beding geldt
afspraken op het gebied van opleiding:	Gedurende dienstverband, plus indien werknemer opleidingskosten moet vergoeden na beëindiging van het dienstverband, gedurende die periode
aanvraag voor opleiding door werknemer:	tot afronding/afbreking opleiding
afspraken over de loopbaan:	tot realisatie
ziektekosten:	duur verzekering tot vertrek
loonbeslag:	tot opheffing beslag
brieven op het gebied van jubilea:	tot beëindiging dienstverband
correspondentie directie/PZ/directe chef:	tot beëindiging van het dienstverband en eventueel afhankelijk van ontslagsituatie tot twee jaar daarna
Logfiles Computersystemen	Max. **6 maanden**
E-mail / Internet-monitoring	Max. **6 maanden**
Backup gegevens	Max. **3 maanden**
Logfiles	Max. **6 maanden** nadat het recht op toegang is vervallen.