Beleid:	Informatiebeveiliging en privacy	
Uitgiftedatum:	7 mei 2018	
☑ **Definitief** ☐ **Concept**		
Versienummer:		
Datum vaststelling directie overleg:	27 september 2018	

ACHTERGROND

Informatie is overal. Het is overal om ons heen te vinden: op ons bureau, in dossiers, op ons computerscherm, aan het prikbord, op social media noem maar op. Hoewel we ons er misschien niet altijd van bewust zijn, zijn we als dienstverlener continu bezig met het verzamelen, bewerken, creëren en het verspreiden van informatie. Het betreft informatie over SGL, over medewerkers en vrijwilligers, maar voornamelijk informatie over onze cliënten.

Informatieverwerking beschrijft in één woord al onze activiteiten. SGL is hierdoor sterk afhankelijk van informatie en de informatieverwerkende processen/systemen. Deze componenten staan voortdurend bloot aan dreigingen zoals diefstal, vernieling, spionage, verlies, storingen, fouten en ongelukken. De gevolgen kunnen desastreus zijn. Om de continuïteit van onze onderneming te kunnen blijven waarborgen, moet SGL zich als collectief inspannen voor de beveiliging van informatie en informatieverwerkende systemen.

SGL stelt zich ten doel optimale dienstverlening te bieden aan onze cliënten, waarbij inspanningen ter behoud van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie als vanzelfsprekend worden geacht. De infrastructurele voorzieningen (hard- en software), de organisatie, processen en procedures moeten hierin faciliteren. SGL wil daarbij ook aan alle vigerende wet- en regelgeving op dit gebied, in het bijzonder de Algemene Verordening Gegevensbescherming (AVG), voldoen.

Dit betekent dat op het gebied van informatiebeveiliging en privacy:

- SGL zich inspant om een "veilige" zorgomgeving voor cliënten en een "veilige" werkomgeving voor medewerkers en vrijwilligers te creëren.
- Het management van SGL aan medewerkers handvatten uitreikt voor het beveiligingsbewust handelen.
- Het management van SGL periodiek het managementsysteem voor informatiebeveiliging en privacy beoordelen.
- Het management van SGL instemt met de uitvoering van de beleidsuitgangspunten die in dit beleid zijn vastgelegd.
- Medewerkers, vrijwilligers en cliënten zich bewust moeten zijn van hun eigen verantwoordelijkheden.

Het informatiebeveiligings- en privacybeleid kan worden beschouwd als onderdeel van het SGL-organisatiebeleid. Het biedt medewerkers en vrijwilligers houvast bij de uitvoering van de dagelijkse werkzaamheden, maar verschaft ook duidelijkheid met betrekking tot de algemene en individuele verantwoordelijkheden.

1 INLEIDING

Informatiebeveiliging is van toepassing op alle bedrijfsprocessen. Het heeft betrekking op informatie, informatiesystemen, netwerken, de fysieke omgeving en de mensen die de bedrijfsprocessen van SGL ondersteunen. Vertrouwen is voor SGL de basis om met onze medewerkers, vrijwilligers, cliënten, relaties en partners samen te werken. Dit vraagt om openheid van SGL en van onze medewerkers over de gegevens die wij van onze medewerkers, vrijwilligers en cliënten vragen.

In dit document wordt het beleid van SGL ten aanzien van de bescherming van vertrouwelijkheid, integriteit en beschikbaarheid van haar componenten uiteengezet. Componenten zoals hard- en software en de informatie die door de organisatie wordt verwerkt. Het beleid dient als richtlijn en/of norm bij het selecteren en implementeren van maatregelen en bij de evaluatie van informatiebeveiliging en privacy.

Het doel van het informatiebeveiligings- en privacybeleid is het bieden van sturing en ondersteuning van het management ten behoeve van informatiebeveiligings- en privacy-aspecten. In dit beleid wordt vastgesteld:

- in welke richting en binnen welke kaders informatiebeveiliging en privacy dient plaats te vinden;
- welke rollen belangrijk zijn in het kader van informatiebeveiliging en privacy;
- hoe de verantwoordelijkheden voor informatiebeveiliging en privacy zijn belegd.

Het informatiebeveiligings- en privacybeleid beschrijft de algemene aanpak van SGL op het gebied van informatiebeveiliging en privacy op strategisch niveau. Op lagere niveaus worden meer gedetailleerde beschrijvingen van de aanpak en specifieke beveiligingsmaatregelen gegeven.

De opbouw van dit document is als volgt. In de volgende hoofdstukken wordt ingegaan op informatiebeveiliging en privacy in het algemeen, de doelstelling, reikwijdte en uitgangspunten, et cetera. In hoofdstuk 4 wordt het managementproces beschreven. In hoofdstuk 5 staat de aanpak centraal, gevolgd door het beleid in hoofdstuk 6. Dit beleid wordt afgesloten met het onderdeel kwaliteitsbewaking, dit wordt beschreven in hoofdstuk 7.

2 INFORMATIEBEVEILIGING EN PRIVACY

2.1 Beheer informatiebeveiligingsbeleid

De Functionaris Gegevensbescherming is verantwoordelijk voor het beheer van het informatiebeveiligings- en privacybeleid.

2.2 Werkingsgebied/ Scope

Dit beleid is van toepassing op de gehele SGL-organisatie. Dit beleid is van toepassing op alle bedrijfsprocessen, informatiesystemen, netwerken, toepassingen, locaties en medewerkers onder de noemer SGL.

2.3 Doel

Het doel van *informatiebeveiliging* is het optimaal ondersteunen en beschermen van het primaire proces "Zorg" en de daaraan ondersteunende diensten en systemen. Informatiebeveiliging dient de beveiliging van informatieverwerkende componenten van SGL te waarborgen. Dit bestaat uit:

- Behoud van beschikbaarheid: er voor zorgen dat informatie zoals vereist en wanneer nodig voor de bedrijfsdoelstellingen van SGL beschikbaar zijn.
- Behoud van integriteit: het beschermen van informatie tegen niet geautoriseerde en/of (on)opzettelijke wijzigingen ten behoeve van de juistheid, volledigheid en inhoudelijke betrouwbaarheid van informatie.
- Behoud van vertrouwelijkheid: het beschermen van informatie tegen niet geautoriseerde openbaarmaking.

De doelstelling van *privacy* is het waarborgen van de beveiliging en de rechtmatige verwerking van de persoonsgegevens van medewerkers, cliënten, vrijwilligers en relaties. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende worden beveiligd en worden verwerkt voor het doel waarvoor het is verzameld. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van deze gegevens.

SGL stelt zich ten doel optimale dienstverlening te bieden, waarbij inspanningen ter behoud van beschikbaarheid, integriteit en vertrouwelijkheid van informatie als vanzelfsprekend worden geacht. Het behoud van beschikbaarheid, integriteit en vertrouwelijkheid van informatie is onderdeel van de doelstelling om drie redenen:

1. Het voldoen aan wet- en regelgeving, waaronder de (AVG).
2. Het voldoen aan zakelijke eisen van informatiebeveiliging. Verlies van beschikbaarheid, integriteit en vertrouwelijkheid van informatie leidt direct of indirect altijd tot een kostenpost. Kostenposten zijn niet alleen herstelkosten maar ook imagoschade.
3. Het voldoen aan interne kwaliteitseisen.

Wanneer niet volledig wordt voldaan aan wet- en regelgeving en/of wanneer niet volledig wordt voldaan aan de zakelijke eisen van informatiebeveiliging, loopt SGL een risico. Het doel van informatiebeveiliging is niet het elimineren van deze risico's, maar het herkennen van deze risico's, het nemen van maatregelen tegen deze risico's en het accepteren van een bepaald niveau van restrisico.

Informatiebeveiliging verschaft inzicht in beveiligingsrisico's en beveiligingsincidenten. Door maatregelen te implementeren tracht SGL het risiconiveau en het aantal incidenten te reduceren. Doel hiervan is het bereiken van een risicobewuste, beheersbare bedrijfsvoering.

Het is voor de Raad van Bestuur van SGL van essentieel belang dat cliënten, medewerkers en vrijwilligers kunnen werken in een veilige omgeving waarbij een zorgvuldige en respectvolle omgang met elkaar en met privacygevoelige informatie is gewaarborgd.

De waarde van informatiebeveiliging en privacy voor SGL

Teneinde van waarde te zijn voor SGL, moet informatiebeveiliging haar primaire zorgprocessen en organisatiedoelstellingen ondersteunen. Hierbij staat steeds de cliënt centraal. De uitkomst hiervan is:

- zorgdragen dat mensen en middelen veilig zijn;
- vertrouwen bieden in een zorgvuldige omgang met privacygevoelige informatie;
- het voldoen aan relevante wet- en regelgeving;
- het beschermen en uitbouwen van haar reputatie.

3 BELEID

SGL wil een veilige omgeving bieden waarin optimaal aan goede zorg gewerkt kan worden. Zowel voor cliënten als voor medewerkers als voor vrijwilligers betekent dit dat ze gerust kunnen zijn in het besef dat zorgvuldig en discreet met privacygevoelige informatie wordt omgegaan.

SGL streeft naar openheid in de zorg- en ondersteuning waarbij de zorgprofessional al naar gelang de wensen van de cliënt dit in een open dan wel gesloten setting verzorgd. Concreet betekent dit dat te allen tijde dat de toegang tot privacygevoelige informatie beperkt is tot het begeleidende team en de cliënt zelf en waar benodigd ondersteunende diensten zoals beheer.

De eisen ten aanzien van de zorgprofessional gelden onverkort voor de medewerkers in de ondersteunende diensten. Van medewerkers in de ondersteunende diensten wordt verwacht dat ze inzicht hebben in de aard en de dynamiek van de zorgverlening en de bijbehorende risico's ten aanzien van de privacy waarborgen.

Een veilige omgeving wordt bereikt door teamwork. Iedereen is verantwoordelijk voor zijn eigen handelen en voor elkaar. Het is daarom van groot belang elkaar te helpen en elkaar aan te spreken op onveilig gedrag.

- SGL streeft ernaar te voldoen aan alle, van toepassing zijnde, wet- en regelgeving, zoals Wet Geneeskundige Behandelingsovereenkomst (WBGO), Wet kwaliteit, klachten en geschillen zorg (Wkkgz), Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG), Wet bescherming persoonsgegevens (Wbp) / de Algemene Verordening Gegevensbescherming (AVG).
- SGL voert een actief beleid om het beveiligingsbewustzijn te stimuleren van eenieder die werkzaamheden verricht in naam van SGL.
- SGL hanteert een gedegen inwerkprogramma voor al haar medewerkers met aandacht voor de omgang met privacygevoelige informatie.
- SGL hanteert een clean desk, clear screen beleid.
- SGL hanteert een beleid dat alle cliëntgegevens in Pluriform worden verwerkt.
- SGL hanteert een beleid dat alle medewerkersgegevens in Beaufort/YouForce/Verzuimsignaal worden verwerkt.
- Er wordt geen vertrouwelijke informatie op verwijderbare media zoals USB-sticks opgeslagen.
- Cluster I&A draagt zorg voor het ter beschikking stellen van de benodigde ICT-middelen en de beveiliging daarvan.

Informatiebeveiligingsdoelstellingen

- Informatiebeveiliging wordt gewaarborgd door een managementsysteem dat goed onderhouden en periodiek gereviewed wordt, zodat op basis van aantoonbare resultaten voldaan wordt aan eisen gesteld vanuit de zorgverlening en vanuit relevante regelgeving.
- Het management van SGL draagt het beleid actief uit en verwacht van alle medewerkers dat zij dat ook doen en ieders verantwoordelijkheid daarin neemt.
- Zorgdragen dat incidenten ontdekt, gemeld en afgehandeld worden.
- Zorgdragen dat tekortkomingen afgehandeld worden.
- Het waarborgen van de privacy van de informatie van cliënten.

- Zorgdragen voor bescherming van de informatie en haar onderliggende systemen tegen cybercriminaliteit.
- Zorgdragen dat kwetsbaarheden geïdentificeerd en weggenomen worden.
- Zorgdragen dat informatiesystemen te allen tijde up-to-date zijn.
- Zorgdragen voor de beschikbaarheid van de informatiesystemen.
- Het waarborgen van de privacy van de personeelsinformatie.
- Zorgdragen dat het personeel adequaat getraind is om de aan haar toegewezen informatiebeveiligingstaken en -verantwoordelijkheden te vervullen.
- Zorgdragen dat personeel geschikt is voor de functie waarvoor ze in aanmerking komt vanuit informatiebeveiligingsperspectief.
- Zorgdragen voor bescherming van de informatie en haar onderliggende systemen tegen criminele risico's (diefstal, inbraak).

4 Managementsysteem

4.1 Managementproces

Het managementproces is ingericht op basis van de 'Deming Circle' (Plan – Do – Check – Act). De 'Deming Circle' bevat de volgende aspecten:

- Plan: detectie en inventarisatie van beveiligings- en privacyrisico's en het opstellen van maatregelen.
- DO: de implementatie van relevante (nieuwe) maatregelen.
- Check: controleren van de effectiviteit van de geïmplementeerde maatregelen.
- Act: daar waar noodzakelijk bijsturen van het managementproces en de genomen maatregelen.

Voor de opzet van het managementproces hanteert SGL het geïntegreerd Management Systeem Governance model van voor Informatiebeveiliging en privacy (ISMS). Dit model is gebaseerd op de internationale standaarden voor informatiebeveiliging managementsystemen zoals opgesteld in de ISO27001 door de International Standards Organization (ISO), de NEN 7510:2011 en de richtsnoeren voor de beveiliging van persoonsgegevens zoals deze zijn opgesteld door de Autoriteit Persoonsgegevens (AP).

4.2 Managementverantwoording

Beheersing van kwaliteit en informatiebeveiliging en privacyaspecten wordt bereikt door een stelsel van organisatorische en technische maatregelen. Deze maatregelen betreffen: een strategisch beleid, richtlijnen, procedures, gedragscodes, werkinstructies, een organisatie en controles. Medewerkers dienen bewust te worden gemaakt van het belang van deze maatregelen en daar waar nodig geïnstrueerd te worden.

Hierbij neemt SGL het volgende standpunt in: SGL treft al die maatregelen die noodzakelijk en in economische zin rendabel zijn om de veiligheid van de informatie en het personeel te waarborgen, aan de relevante wet- en regelgeving te voldoen, de continuïteit van de bedrijfsvoering te waarborgen en om de reputatie te beschermen.

De Raad van Bestuur van SGL is verantwoordelijk voor de werking van het managementsysteem en zal via delegatie naar medewerkers de taken en verantwoordelijkheden beleggen voor de implementatie en beheer van maatregelen voortkomend uit dit beleid.

4.3 Medewerkersverantwoording

Alle medewerkers van SGL hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen welke voortvloeien uit dit beleid. Identificatie van incidenten of non-compliance ten aanzien van dit beleid dienen gemeld conform protocol Meldplicht Datalekken.

4.4 Beoordeling en corrigerende maatregelen

SGL zal de maatregelen welke voortkomen uit dit beleid periodiek controleren middels controles en interne en externe audits ten aanzien van (kosten)effectiviteit. Jaarlijks zal de Raad van Bestuur het managementsysteem beoordelen op basis van verzamelde gegevens en informatie. Input voor deze beoordeling is onder andere:

- Registratie van incidenten en non-compliance issues
- Registraties van contrôle, interne en externe audits
- Klanttevredenheidsonderzoeken
- Leveranciersbeoordelingen
- Risicoanalyse output
- Privacy Impact Assessments
- Medewerkerscompetenties
- Bewustwording en training
- Wet- en regelgeving

Op basis van de (tussentijdse) beoordelingen zullen waar mogelijk corrigerende en/of preventieve maatregelen worden doorgevoerd. Corrigerende en preventieve maatregelen kunnen ook voortkomen uit overleggen en bijbehorende rapportages. Op een dusdanige wijze dat de kans op herhaling geminimaliseerd wordt. Of waardoor de doeltreffendheid van het managementsysteem wordt verbeterd en het geleverde product of dienst beter aansluit op de eisen van de klant.

4.5 Documentatie

4.5.1 Gedocumenteerde informatie

SGL draagt zorg voor de verplichte documentatie die binnen de scope van het informatie-beveiliging en privacymanagementsysteem vallen. Daarnaast wordt bepaald welke aanvullende documentatie benodigd is om de effectiviteit van het managementsysteem te borgen. Gedocumenteerde informatie kan zich zowel in het managementsysteem als in operationele systemen bevinden.

4.5.2 Classificatie van gegevens

Voor een effectieve bescherming van de informatie is vereist dat de waarde van de informatie voor de onderneming bekend is. Classificatie van informatie in termen van vereiste vertrouwelijkheid, integriteit en beschikbaarheid:

- informeert het management en medewerkers over wat moet worden beschermd en hoe informatiemiddelen op een standaard manier kunnen worden beschermd;
- toont de waarde van middelen aan medewerkers, zodat het bewustzijn van beveiliging binnen hun dagelijkse werkzaamheden wordt gestimuleerd;
- stelt SGL in staat te voldoen aan eventuele wettelijke en contractuele verplichtingen.

De eigenaar van de informatie blijft verantwoordelijk voor het up-to-date houden van de identificatie van informatiemiddelen en de toegekende waarde van elk van de geïdentificeerde middelen.

5 AANPAK VAN INFORMATIEBEVEILIGING / PRIVACY

5.1 Informatiebeveiliging / Risicomanagement

5.1.1 Risicobewustzijn

Risicobewustzijn van alle medewerkers van SGL is de sleutel tot een effectieve informatiebeveiliging. Risicobewustzijn wordt volledig ondersteund door de Raad van Bestuur van SGL en zal gestimuleerd worden door middel van training en publicaties via onder meer Intranet, posters en ons personeelsmagazine Dichtbij SGL. Het risicobewustzijn wordt ook ondersteund door het opstellen en naleven van reglementen en zal indien nodig ook aandacht krijgen in functiebeschrijvingen en arbeidscontracten of inhuurovereenkomsten.

5.1.2 Risico-identificatie

Via een vastgestelde methodiek worden mogelijke dreigingen, informatiebeveiliging en privacyrisico's geïdentificeerd en geïndexeerd. Het management zal de resultaten hieruit voortkomend beoordelen en 'zo kosten effectief mogelijk' maatregelen implementeren ter vermindering van het risico tot een acceptabel niveau.

5.2 Beperkte toegang

Toegang tot informatie en IT-faciliteiten zal op basis van 'need to know' worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. Dit is één van de essentiële principes van veilig informatiebeheer. Toegang tot informatiesystemen wordt geïnitieerd door de leidinggevende van de medewerker op basis van toegekende autorisaties en de medewerkersrol. Na het accorderen door de informatie- of informatiesysteemeigenaar zullen de autorisaties worden toegekend.

5.3 Informatie eigendom

ICT-middelen die aan SGL-medewerkers beschikbaar worden gesteld, dienen voor zakelijke doeleinden toegepast te worden. Opgeslagen en verwerkte informatie van of voor SGL op systemen van de onderneming blijft te allen tijde eigendom van de SGL-organisatie. De internationale en lokale privacywetgeving zal worden gehandhaafd wanneer een beroep wordt gedaan op eigendomsrechten.

5.4 ICT-infrastructuur

SGL heeft een ICT-infrastructuur geïmplementeerd voor de eigen bedrijfsonderdelen en locaties die onderlinge interne communicatie en samenwerking met partners, klanten en medewerkers op afstand mogelijk maakt. Deze ICT-infrastructuur is deels (end-devices) eigendom van SGL en voor een deel in beheer en/of eigendom van een aantal externe partijen zoals onder andere Detron. Voor bepaalde diensten wordt gebruik gemaakt van externe publieke netwerken zoals het internet. Hierdoor zijn er diverse beveiligings- en beheersmaatregelen geïmplementeerd om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen.

6 BELEIDSKADERS

6.1 Vertrouwen en veiligheid

Vertrouwen is voor SGL de basis om met onze medewerkers, cliënten, relaties en partners samen te werken. Dit vertrouwen vraagt om openheid van SGL over de gegevens die wij van onze medewerkers, vrijwilligers, cliënten en relaties vragen. Maar ook om veiligheid van diezelfde gegevens bij ons als werkgever of aanbieder van onze producten en diensten. SGL

gaat daarbij zorgvuldig om met gegevens en zorgt voor een passend niveau van beveiliging en zorgt ervoor dat elke verwerking van gegevens voldoet aan de toepasselijk wet- en regelgeving.

6.2 Informatiebeveiliging

Informatie, informatiesystemen, toepassingen en netwerken van SGL dienen in voldoende mate beschikbaar te zijn, dienen volledige en juiste informatie te bevatten en dienen uitsluitend toegankelijk te zijn voor rechtmatige gebruikers. De informatie, informatiesystemen, toepassingen en netwerken moeten in staat zijn bedreigingen voor hun beschikbaarheid, integriteit en vertrouwelijkheid te weerstaan en moeten zich kunnen herstellen bij het optreden van incidenten en calamiteiten.

Om hieraan te kunnen voldoen zal SGL het volgende doen:

- SGL zal alle componenten op het gebied van hard- en software en informatie beschermen die onder haar beheer vallen. Dit wordt bereikt door het implementeren en beheren van een uitgebalanceerd pakket technische en organisatorische beveiligingsmaatregelen.
- SGL zal in verhouding tot de risico's voor haar componenten effectieve en efficiënte beveiliging bieden.
- SGL zal het informatiebeveiligingsbeleid op een consistente, tijdige, effectieve en efficiënte manier implementeren en beheren.
- SGL zal voor alle bedrijfskritieke informatiesystemen, toepassingen en netwerken een systeembeveiligingsbeleid opstellen. Hierin komen aan bod:
  - De autorisaties voor het gebruik van het systeem;
  - Een beschrijving van beveiligingsmaatregelen die van toepassing zijn op het systeem;
  - De verantwoordelijkheden en bevoegdheden voor het systeem;
  - Een continuïteitsplan voor het systeem.
- SGL zal zich inspannen om haar medewerkers (de gebruikers van informatiesystemen, toepassingen en netwerken) uitleg te geven over beveiliging en hun verantwoordelijkheden en om het noodzakelijke beveiligingsbewustzijn onder de medewerkers te creëren. Hiertoe zal een bepaalde vorm van training worden toegepast.
- SGL zal aan alle medewerkers duidelijk maken dat onverantwoordelijke en/of ongepaste daden kunnen leiden tot disciplinaire maatregelen.
- SGL zal sluitende afspraken maken met externe relaties / leveranciers inzake informatiebeveiliging.

Waar van toepassing zal SGL zich houden aan:

- Nederlandse en Europese wet- en regelgeving.
- Gedrag en beroepsregels van de beroepsorganisaties van de medewerkers van SGL.
- Gedrag en fatsoensnormen van het maatschappelijk verkeer.

6.3 Gegevens en privacy

Dit beleid is van toepassing op alle gegevens die SGL verzamelt en verwerkt van medewerkers, cliënten, relaties en partners. SGL is de verantwoordelijke voor de verwerking van persoonsgegevens zoals beschreven in dit beleid.

Doeleinden

SGL hecht veel waarde aan de bescherming van uw privacy. Men kan er op vertrouwen dat wij:

- Werken naar de letter en geest van de privacywet- en regelgeving.
- Gegevens veilig en zorgvuldig verwerken.
- Gegevens niet doorgeven of verkopen aan derden voor commerciële of charitatieve doeleinden.
- Wettelijke rechten respecteren.
- Alleen samenwerken met partijen die dezelfde uitgangspunten hanteren.
- Vragen over privacy eerlijk zullen beantwoorden.

Verwerking (bijzondere) persoonsgegevens

Persoonsgegevens zijn gegevens die ofwel direct over iemand gaan ofwel naar iemand te herleiden zijn. Denk hierbij aan naam, geboortedatum, adres, gegevens over gezondheid en dergelijke. Wij verwerken deze gegevens om op een goede wijze van dienst te kunnen zijn of om te voldoen aan onze wettelijke verplichtingen.

Persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is. De verwerking moet plaatsvinden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen en moet beperkt zijn tot hetgeen noodzakelijk is. Daarbij is het ook belangrijk dat de persoonsgegevens juist zijn en zo nodig worden geactualiseerd, niet langer worden bewaard dan noodzakelijk en toegestaan en afdoende beschermd (artikel 5 AVG). Wat betreft de bewaartermijn wordt verwezen naar de SGL-beleidsnotitie "Beheer van registratie".

Verwerking van de persoonsgegevens is rechtmatig als de betrokkene daarvoor toestemming heeft verleend, of de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waar betrokkene partij bij is, of de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting, het vitale belang van de betrokkene te beschermen, of voor het vervullen van een taak van algemeen belang dan wel voor de behartiging van de gerechtsvaardigde belangen van de verwerkings-verantwoordelijke of van een derde (artikel 6 AVG).

Bijzondere persoonsgegevens, zoals bijvoorbeeld gegevens over de gezondheid of BSN-nummer, mogen alleen worden verwerkt als er aan nog aan een aanvullende voorwaarde is voldaan, zoals bijvoorbeeld het verlenen van gezondheidszorg aan betrokken of op basis van verplichtingen op het gebied van het arbeidsrecht en het sociale zekerheidsrecht ten aanzien van betrokkene (artikel 9 AVG).

Toegang tot gegevens

SGL schakelt bij de uitvoering van haar dienstverlening derden in. Voor zover deze derden bij het uitvoeren van de betreffende diensten en bedrijfsactiviteiten gegevens verwerken, doen zij dit in hoedanigheid van "bewerker" voor SGL en heeft SGL de vereiste technische en organisatorische maatregelen getroffen om te verzekeren dat gegevens uitsluitend voor bovenstaande doeleinde worden gebruikt. Uitsluitend indien SGL hiertoe wettelijk is verplicht, worden persoonsgegevens verstrekt aan toezichthouders, fiscale autoriteiten en opsporingsinstanties.

Beveiliging van gegevens
Men mag van ons verwachten dat SGL er alles aan zal doen om privacy te waarborgen. Uiteraard houden wij ons aan de wet- en regelgeving. Alle SGL-medewerkers hebben geheimhoudingsplicht. SGL gaat uiterst zorgvuldig om met persoonsgegevens. Wij hebben verschillende technische en organisatorische maatregelen genomen om persoonsgegevens te beveiligen. Zo beveiligen wij onze systemen en applicaties volgens de geldende standaarden voor informatiebeveiliging. Cluster I&A van SGL is op moment van schrijven bezig met het voldoen aan de NEN 7510:2011 certificering. Bovendien bewaren wij de verzamelde gegevens niet langer dan noodzakelijk is. Hoe lang dat precies is, kan in verschillende wetten zijn vastgelegd en hangt af van het specifieke gegeven en het doel waarvoor wij gegevens verwerken.

Vragen en verzoeken om inzage, correctie en verwijdering
Wanneer iemand informatie wil, over zichzelf, kunnen wij deze informatie pas geven als voldoende duidelijk is wie diegene is (identificeren) en ook daadwerkelijk de persoon is die hij zegt te zijn (authenticeren). Wij verstrekken geen gegevens over de telefoon of via e-mail zonder dat wij zeker weten dat wij de betreffende persoon aan de telefoon hebben of een e-mail van zijn e-mailadres afkomstig is.

Personen hebben een aantal rechten met betrekking tot hun persoonsgegevens:
- Recht op inzage in door ons van hem vastgelegde gegevens.
- Recht op indienen van een verzoek tot correctie of verwijdering van zijn gegevens.
- Recht om bezwaar te maken (verzet) tegen bepaalde wijze van gebruik van zijn gegevens.

In sommige gevallen kunnen of mogen wij geen wijziging of verwijdering doorvoeren. Bijvoorbeeld als dat in strijd met de wet is. Een verzoek tot inzage of correctie kunt u indienen bij onze Functionaris Gegevensbescherming en via e-mail pmeiser@sgl-zorg.nl. Binnen 15 werkdagen zal deze met een reactie komen.

7 KWALITEITSBEWAKING

7.1 Communicatie

In de communicatie van dit beleid staat centraal de bewustwording van het eigen personeel (en ingehuurde derden), de naleving van de regels en richtlijnen. Om dit te bewerkstelligen zullen er gedragsregels opgesteld en gecommuniceerd worden zodat medewerkers weten wat er van hun verwacht wordt, welke risico´s er zijn en welke rechten en plichten ze hebben. Veranderingen en aanpassingen in het managementsysteem worden door het management beoordeeld en intern gecommuniceerd, indien nodig ook naar relevante externe partijen.

Het management bepaalt:
- wat gecommuniceerd wordt;
- wanneer gecommuniceerd wordt;
- met wie gecommuniceerd wordt;
- wie de communicatie uitvoert en;
- welke processen door de communicatie beïnvloed worden.

7.2 Borging

Borging vindt plaats door middel van vastlegging van de overeengekomen werkwijze in procesbeschrijvingen, richtlijnen, een gedragscode, procedures, werkinstructies en tooling. Deze dienen voor alle medewerkers toegankelijk te zijn en zullen via Intranet verspreid worden, zodat in het geval van incidenten en calamiteiten deze snel en eenduidig toegankelijk zijn.

7.3 Geldigheid

De Raad van Bestuur is eigenaar van dit beleidsdocument. Het beheer, opstellen en actueel houden van het beleidsdocument is de verantwoordelijkheid van de Functionaris Gegevensbescherming.

Dit beleid is drie jaar geldig en wordt minimaal een keer per jaar geëvalueerd met het oog op:

- De toereikendheid en de tactische en operationele uitvoering ervan;
- De stand van de techniek (beveiliging en bedreiging);
- Voortschrijdend inzicht;
- Veranderende wet- en regelgeving of organisatie.

Op grond van de jaarlijkse beoordeling, veranderende wet- en regelgeving of door andere omstandigheden, kan dit beleid tussentijds bijgesteld worden.

7.4 Naleving

Naleving van het beleid wordt gecontroleerd. Niet naleving van het beleid kan disciplinaire maatregelen tot gevolg hebben, conform SGL-beleid en regelgeving.