Privacy- en informatiebeveiligingsbeleid

SRK Rechtsbijstand B.V.

Versie: 1.2

Status: Definitief
Auteurs: Jan Bernard ter Horst, Marco Split

Vastgesteld door de Stuurgroep Informatiebeveiliging en Privacybescherming van de stichting SRK op: 25-05-2018
Vastgesteld door de directie van SRK Rechtsbijstand B.V. op: 13-08-2019

Privacybeschermings- en Informatiebeveiligingsbeleid	
Organisatie: SRK Rechtsbijstand B.V.	Procesnummer: n.v.t.
Eigenaar: Voorzitter Stuurgroep Privacy en Informatiebeveiliging	Versie: 1.2
Versiedatum: 13 augustus 2019	Pagina's: 18

Versie	Omschrijving aanpassingen	Naam	Datum
0.1	Eerste concept samenvoeging IB en privacybeleid t.b.v. review	Jan Bernard ter Horst	07-02-2018
0.2	Na verwerking opmerkingen JB	Peter Hoogenberg	30-03-2018
0.3	Reactie JHO op versie 0.2	Jan Bernard ter Horst	16-05-2018
0.4	Review door ISO Marco	Marco Spilt	17-05-2018
1.0	Versie 1.0 goedgekeurd door stuurgroep Informatiebeveiliging en Privacybescherming	Marco Spilt	25-05-2018
1.1	Review vanuit SRK Rechtsbijstand B.V.	Leon Juchter van Bergen Quast	06-08-2019
1.2	Vastgesteld door de directie van SRK Rechtsbijstand B.V.	Peter Leermakers	13-08-2019

Revisie
Tussentijdse wijzigingen in het beleid worden direct verwerkt. Dit beleid wordt jaarlijks in augustus volledig gereviseerd.

Vertrouwelijkheid
Bedrijfskritisch

Change betrokkenen
Stuurgroep Privacy en Informatiebeveiliging

Vindplaats voor de eigenaar
brandmr.sharepoint.com/sites/privacyenib/Gedeelde%20documenten/Forms/AllItems.aspx

Voor medewerkers te raadplegen
Intranet

Voor cliënten te raadplegen
Publieke website

Inhoudsopgave

Hoofdstuk 1 – Inleiding, doel/opzet en kaders

1.1 Inleiding

SRK Rechtsbijstand B.V. (hierna: SRK) heeft als (statutair) doel de belangen te behartigen van particulieren en bedrijven met een rechtsbijstandverzekering bij één van de aangesloten verzekeraars. Bij onze juridische dienstverlening wordt veel informatie opgevraagd, opgeslagen en uitgewisseld. Daarnaast verwerkt SRK informatie, waaronder persoonsgegevens, als werkgever en als organisatie, in het kader van de bedrijfsvoering.

De verwerking van informatie geschiedt hoofdzakelijk langs digitale wegen en systemen. Ontwikkelingen gaan snel en de infrastructuur, diensten, applicaties en werkwijzen veranderen. Datzelfde geldt voor de digitale bedreigingen zoals toenemende afhankelijkheid van IT, storingen en cybercrime. De vraag van de klant ontwikkelt zich door dit soort ontwikkelingen ook, evenals de eisen die we moeten stellen aan de organisatie, werkwijzen en techniek.

Onze klanten, samenwerkingspartners, medewerkers en andere betrokkenen mogen op basis van de aard van onze diensten en wet- en regelgeving vertrouwen op een zorgvuldige en behoorlijke omgang met hun gegevens en belangen. SRK heeft de visie te allen tijde zoveel mogelijk transparant te communiceren over haar gegevensverwerkingen.

Privacybescherming en informatiebeveiligingsbeleid is een verantwoordelijkheid van ons allemaal: Directie, (lijn)management en medewerkers. SRK vindt het belangrijk dat iedere medewerker zich bewust is (awareness) van de noodzaak om zorgvuldig en behoorlijk met informatie en persoonsgegevens om te gaan en hier ook naar handelt.

Het beleid heeft betrekking op werkprocessen, systemen en procedures, maar ook op de besluiten die worden genomen en in ons dagelijks handelen en geeft aan op welke wijze we privacybescherming en informatiebeveiliging binnen SRK vormgeven en borgen. Het bevat de uitgangspunten voor en beschrijving van de maatregelen die SRK daartoe neemt met het oog op de beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens en informatie en van onze dienstverlening als geheel.

1.2 Doel en opzet van privacybeschermings- en informatiebeveiligingsbeleid

Privacybeschermings- en informatiebeveiligingsbeleid heeft tot doel te voorzien in alle maatregelen die nodig zijn om voldoende bescherming en beveiliging te bieden en voortdurend in stand te houden, het signaleren van risico's en deze in zowel tijd als omvang te minimaliseren. Maatregelen is in dit verband het verzamelbegrip voor onder meer processen, procedures, verantwoordelijkheden, middelen, afspraken etc. die daarbij worden ingezet of ingericht en die deel uitmaken van het beleid als geheel.

Dit beleidsdocument biedt houvast en duidelijkheid over de wijze waarop privacybescherming en informatiebeveiliging binnen SRK is vormgegeven en wordt geborgd. Het beschrijft niet alle maatregelen zelf, maar geeft het kader en verwijst naar de (deel)verantwoordelijken voor bepaalde maatregelen en de vindplaatsen van die maatregelen.

Privacybescherming en Informatiebeveiliging is een procesmatige activiteit en is integraal onderdeel van het risicomanagement van SRK. De juiste mentaliteit, integriteit en awareness wordt in deze als basishouding van alle medewerkers verwacht.

Privacybescherming in combinatie met Informatiebeveiliging beschermt betrokkenen tegen onrechtmatige verzameling en verwerking van hun persoonsgegevens en beschermt informatiemiddelen die ook persoonsgegevens bevatten tegen een groot aantal risico's, zoals, verlies, operationele discontinuïteit, misbruik, ongeoorloofde openbaarmaking en ontoegankelijkheid van informatie. Daarmee beschermt het ook tegen de risico's van mogelijke imago schade die SRK en haar opdrachtgevers/verzekeraars daar door kunnen lijden

Het beschermt ook tegen de steeds toenemende juridische aansprakelijkheidsrisico's waarmee organisaties worden geconfronteerd als gevolg van onjuistheden in informatie of verlies van informatie, dan wel het ontbreken van de nodige zorgvuldigheid in de bescherming, verzameling en verwerking van informatie.

Speciale aandacht hierbij voor de Algemene Verordening Gegevensbescherming, welke wettelijk per 25 mei 2018 van kracht zal zijn. Hieruit volgt een uitbreiding en versterking van de privacyrechten, waarbij de verantwoordelijkheid nadrukkelijker bij organisaties komt te liggen.

Een juiste vormgeving en invulling van privacybescherming en informatiebeveiliging is gezien de aard van onze activiteiten en bedrijfsprocessen dan ook geen 'moeten': het is de intrinsieke ambitie van SRK omdat het ondersteunt bij het daadwerkelijk realiseren van de doelstellingen op het gebied van innovatie, slagkracht, betrouwbaarheid en natuurlijk de continuïteit van SRK als onderneming.

In hoofdstuk 2 zijn de beginselen en regels inzake *privacybescherming* uitgewerkt in beleidsmaatregelen.
In hoofdstuk 3 is dat het geval voor *informatiebeveiliging.*

1.3 Kaders

De eisen die aan privacybescherming en informatiebeveiliging worden gesteld, of de resultaten daarvan komen voort uit verschillende bronnen, waaronder in ieder geval:

1. Regels voor de beroepsgroep van advocaten en kwaliteitscode rechtsbijstand van het Verbond van Verzekeraars
2. De Algemene Verordening Gegevensbescherming;
3. De Uitvoeringswet Algemene Verordening Gegevensbescherming;
4. Handleidingen en richtsnoeren van het Ministerie en Toezichthouder;
5. De dienstverleningsovereenkomsten met verzekeraars;
6. Toetsingskader informatiebeveiliging DNB;
7. De polisvoorwaarden tussen verzekeraars en klanten die een beroep doen op SRK.

Dit document benoemt de belangrijkste beginselen en regels, maar ziet vooral op beschrijving van de maatregelen en de wijze waarop verantwoordelijkheden zijn belegd.

Hoofdstuk 2 – Beleid inzake de bescherming van Privacy

In dit hoofdstuk worden de uitgangspunten, regels en maatregelen ten behoeve van de bescherming van privacy beschreven.

2.1 Regels

2.1.1. Algemeen

De regels die de AVG stelt zijn weliswaar omvangrijk, maar zijn gebaseerd op heldere leidende beginselen die daarmee ook de beginselen voor dit privacybeschermingsbeleid vormen:

- Verwerking van persoonsgegevens is rechtmatig, behoorlijk en transparant; belangrijk onderdeel hiervan zijn de grondslagen van art 6 AVG;
- Persoonsgegevens worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden verzameld en vervolgens niet op onverenigbare wijze verwerkt (doelbinding);
- Persoonsgegevens zijn adequaat en ter zake dienend en blijven beperkt tot die gegevens die noodzakelijk en toereikend zijn voor de doeleinden waarvoor zij worden verwerkt (proportionaliteit);
- Persoonsgegevens zijn juist en worden zo nodig gecorrigeerd of geactualiseerd;
- Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden bewaard noodzakelijk is;
- Persoonsgegevens worden door passende technische of organisatorische maatregelen op een dusdanige manier verwerkt dat een passende beveiliging gewaarborgd is;
- persoonsgegevens worden verwerkt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke, die kan aantonen dat verwerking voldoet aan de bepalingen van de verordening.

2.1.2. Aandachtspunten uit de AVG

De verwerking van sommige soorten gegevens kennen eigen voorwaarden en uitzonderingen in de AVG. Het meest van belang binnen de rechtshulpverlening zijn de:

- *bijzondere persoonsgegevens*, zie art. 9 AVG;
- *strafrechtelijke gegevens*, zie art. 10 AVG;
- *gegevens die niet zijn verkregen van betrokkenen zelf*, zie art. 14 AVG.

2.1.3. Rechtshulpverlening

De (beroeps)regels voor advocaten en rechtshulpverleners (kwaliteitscode rechtsbijstand van het Verbond van Verzekeraars) brengen over het algemeen dezelfde verplichtingen met zich mee of kennen een vergelijkbare strekking als de regels van de AVG. Het belang van de klant staat daarbij voorop. De AVG biedt ruimte voor afwegingen en afwijkingen, waarbij beginselen van proportionaliteit en van groot belang zijn. Als een conflict van plichten ontstaat of wordt ervaren, moeten deze worden afgewogen en moet de beslissing toetsbaar zijn. De individuele advocaat of rechtshulpverlener legt belangrijke afspraken conform de gedragsregels vast in het dossier. Op organisatieniveau worden besluiten hieromtrent vastgelegd in het privacy besluiten register.

2.1.4. Verantwoordingsplicht

De verantwoordingsplicht is in art. 5 lid 2 AVG vastgelegd en betekent dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de verplichtingen uit de AVG, die in de kern in lid 1 van dat artikel zijn opgenomen en samengevat. De verwerkingsverantwoordelijke moet naleving van deze verplichtingen kunnen aantonen.

2.2 Categorieën van verwerkingen, verwerkingenregister en verantwoordelijken

SRK kent verschillende groepen, in AVG-termen categorieën, van verwerkingen. Verwerkingen vinden plaats in het kader van een doel en dat doel hangt nauw samen met het doel van die functies in de organisatie.

Alle categorieën van verwerkingen zijn beschreven in het verwerkingenregister, zoals verplicht moet worden bijgehouden overeenkomstig art. 30 AVG. Daarin, of in een eigen afzonderlijk protocol, worden zo nodig de afwegingen die SRK bij de verwerking maakt beschreven. Op die wijze kan per type verwerking ook de basis worden gelegd voor of uitvoering worden gegeven aan de documentatieplicht

Hieronder worden de categorieën van verwerkingen benoemd en kort beschreven en wordt ook de voor de betreffende verwerking verantwoordelijke functionaris aangewezen.

A. Verwerkingen in het kader van de Rechtshulpverlening
De geheimhoudingsplicht en overige verplichtingen van advocaten jegens hun cliënten vormen het leidend kader voor de verwerking van (persoons)gegevens in het kader van de rechtshulpverlening. In zoverre leiden de gedragsregels die binnen de rechtshulpverlening gemeengoed zijn en de AVG over het algemeen tot dezelfde uitkomst, norm of afwegingen.

Iedere rechtshulpverlener heeft een eigen professionele verantwoordelijkheid en zal overeenkomstig de eisen die aan de beroepsgroep worden gesteld (persoons)gegevens slechts delen, voor zover dat de wens en/of in het belang van de klant is. Daarin liggen doel van de verwerking en de grondslag ervan al besloten. Belangrijke verwerkingen zijn die van persoonsgegevens van klanten, wederpartijen en getuigen.

Deze verwerkingen zijn beschreven in het verwerkingenregister.
Verantwoordelijk voor naleving en onderhoud is het management van de rechtshulpverlening.

B. Verwerkingen in het kader van de uitvoering van de verzekeringsovereenkomst
SRK voert de verplichtingen uit de verzekeringsovereenkomst uit. Daartoe heeft SRK informatie nodig van de verzekeraar over de persoon van de verzekerde, contactgegevens en gegevens over de verzekering. Met dat doel informeert de verzekeraar SRK en tot daar is de verzekeraar verwerkingsverantwoordelijke.

SRK is verwerkingsverantwoordelijke, wanneer SRK rechtshulp verleent en daarmee zelf doel van en de middelen voor de verwerking van persoonsgegevens bepaalt (art. 4 lid 7 AVG). In die hoedanigheid verwerkt SRK ook gegevens aan de verzekeraar met de in de polisvoorwaarden omschreven doelen.

Deze verwerkingen zijn beschreven in het verwerkingenregister.
Verantwoordelijk voor naleving en onderhoud is Operationeel Manager SRK Rechtsbijstand B.V.

C. Verwerkingen in het kader van de rol van SRK als werkgever
Persoonsgegevens van sollicitanten, actieve- en inactieve medewerkers en ingehuurde krachten worden door de afdeling HRM bijgehouden in een wervings/personeelsdossier en voor verschillende doelen verwerkt.

Deze doelen en verwerkingen zijn omschreven in het privacy protocol en uitgewerkt in het verwerkingenregister.
Verantwoordelijk voor naleving en onderhoud van het privacy protocol en verwerkingenregister is de HR Business Partner.

D. Verwerkingen in het kader van de organisatie en bedrijfsvoering van SRK
Diverse verwerkingen zijn of kunnen worden ingericht ten behoeve van de algemene bedrijfsvoering van SRK. Daarbij valt te denken aan toegangsbeheer, camerabewaking, bezoekersregistratie, etc.

Deze verwerkingen zijn uitgewerkt in het verwerkingenregister.
Verantwoordelijk voor naleving en onderhoud zijn de Officemanagers.

E. Overige Verwerkingen
Eventuele overige verwerkingen worden in het verwerkingenregister beschreven. Waar van toepassing, wordt ook de verantwoordelijke functionaris aangewezen.

2.3 Toegang tot persoonsgegevens en Geheimhouding

2.3.1. Toegang tot persoonsgegevens

Toegang tot informatie en persoonsgegevens wordt verstrekt indien en voor zover dat nodig is voor de uitoefening van de functie, werkzaamheden of opdracht en voor de duur daarvan.
Iedere leidinggevende is verantwoordelijk voor toekenning en intrekking van de (juiste) toegangsrechten en handhaving van de uitgangspunten daarbij. De Functionaris voor Gegevensbescherming ziet toe op de naleving van procedures en het beleid hieromtrent.

2.3.2. Geheimhoudingsplicht, geheimhoudingsverklaring

Met het oog op de bescherming van persoonsgegevens stelt SRK als voorwaarde aan iedere medewerker die toegang heeft tot informatie dat deze zich middels een verklaring verplicht tot geheimhouding van alle persoonsgegevens en andere informatie waarvan redelijkerwijs het belang voor SRK of derden van vertrouwelijke omgang ermee kan worden begrepen.

De geheimhoudingsplicht wordt ook opgelegd aan tijdelijke en/of externe krachten en/of partijen die op welke wijze ook bij de uitvoering van de dienstverlening of bedrijfsvoering van SRK zijn betrokken.

2.4 Rechten van betrokkenen

De AVG voorziet in de volgende rechten van betrokkenen:

1. Recht op informatie over de verwerking (zie art. 13 en art. 14)
2. Recht van inzage (zie art. 15 AVG);
3. Recht op rectificatie (zie art. 16 AVG);
4. Recht op vergetelheid (gegevenswissing) (zie art. 17 AVG);
5. Recht op beperking van de verwerking (zie art. 18 AVG);
6. Recht op dataportabiliteit (overdraagbaarheid gegevens) (zie art. 20 AVG);
7. Recht van bezwaar tegen verwerking (zie art. 21 AVG);
8. Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profiling (zie art. 22 AVG).

Ten aanzien van punt 8, inzake het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, doet SRK dit alleen overeenkomstig de in artikel 22 lid 2 sub a AVG gestelde uitzondering, vanwege de noodzakelijkheid in verband met de totstandkoming of uitvoering van een overeenkomst. SRK zorgt hier voor de passende maatregelen ter bescherming van de rechten, vrijheden en gerechtvaardigde belangen van een betrokkene. Waaronder ten minste het recht op menselijke tussenkomst vanuit SRK, het recht van de betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten. SRK stelt voor de verwerking van persoonsgegevens in dit kader ook een gegevensbeschermingseffectbeoordeling op.

De procedure waarmee SRK invulling geeft aan de uitoefening van de rechten van betrokkenen (verzekerden, tegenpartijen en getuigen) is beschreven en gepubliceerd op de openbare website bij het privacy statement. De informatie en procedures waarmee SRK invulling geeft aan de rechten van medewerkers zijn beschreven en gepubliceerd op intranet. Verantwoordelijk voor naleving en onderhoud ligt voor verzekerden, tegenpartijen en getuigen bij de Compliance Officer en voor medewerkers bij de HR Business Partner.

2.5 De functionaris voor gegevensbescherming (FG)

2.5.1. Instelling Functionaris voor Gegevensbescherming

SRK verwerkt veel persoonsgegevens, waaronder op een aantal rechtsgebieden ook veel bijzondere persoonsgegevens. Dat zijn vooral medische gegevens in letselschade- en arbeidsrecht/sociaalverzekeringszaken.

Als SRK “hoofdzakelijk [zou zijn] belast met grootschalige verwerking van bijzondere categorieën van gegevens”, zou op grond van de AVG de verplichting bestaan een functionaris voor gegevensbescherming te benoemen (art. 37 AVG). Het criterium “hoofdzakelijk” wordt niet geconcretiseerd in de AVG.

Vanwege het belang van zorgvuldige omgang met persoonsgegevens in zowel het kader van de AVG, als in het kader van onze professionele activiteiten, kiest SRK vrijwillig voor het benoemen van een functionaris voor gegevensbescherming (FG).

2.5.2. Taken van de Functionaris voor de Gegevensbescherming

De taken van de FG zijn beschreven in art. 39 van de AVG en zijn samen te vatten als de verantwoordelijkheid te informeren en adviseren over de AVG, het toezien op de naleving ervan, in voorkomende gevallen het adviseren of bijstaan van de organisatie bij gegevensbeschermingseffectbeoordeling en optreden als aanspreekpunt voor de Autoriteit Persoonsgegevens.

Om deze taken naar behoren te kunnen uitvoeren, voorziet SRK in voldoende informatie, tijd en ruimte om deze taken te vervullen. Daartoe zal de FG bijvoorbeeld:

- regelmatig worden uitgenodigd om aan vergaderingen van het management deel te nemen;
- worden betrokken/geraadpleegd bij beslissingen met gevolgen voor gegevensbescherming en van de relevante informatie daarbij worden voorzien, om hem in staat te stellen passend advies te geven;
- worden geïnformeerd over eventuele beslissingen die in afwijking van zijn advies zijn genomen en kennis kunnen nemen van de onderbouwing van de beslissing, zodat e.e.a. opnieuw kan worden afgewogen en/of gedocumenteerd;
- onmiddellijk geraadpleegd te worden indien zich een datalek of ander incident zou voordoen;
- voldoende steun krijgen qua financiële middelen, infrastructuur, toegang tot personen, diensten en informatie, opleiding, etc.

2.6 De gegevensbeschermingseffectbeoordeling (PIA of DPIA)

2.6.1 wanneer en hoe?

In gevallen van wijzigingen in de manier waarop persoonsgegevens worden verwerkt, moet worden overwogen of de nieuwe werkwijze of verwerking een risico inhoudt. In art. 35 van de AVG is het als volgt omschreven:

1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.
2. Wanneer een functionaris voor gegevensbescherming is aangewezen, wint de verwerkingsverantwoordelijke bij het uitvoeren van een gegevensbeschermingseffectbeoordeling diens advies in.

De Autoriteit Persoonsgegevens heeft voor de uitvoering van een gegevensbeschermingseffectbeoordeling richtlijnen gepubliceerd: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf

2.6.2 Criteria

Als vuistregel is als criterium geformuleerd dat een verwerkingsverantwoordelijke een DPIA moet uitvoeren als de verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

1. Beoordelen van mensen op basis van persoonskenmerken, zoals profiling, beroepsprestaties, gezondheid, economische situatie, betrouwbaarheid of gedrag etc.;
2. Geautomatiseerde beslissingen, die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben;
3. Stelselmatige en grootschalige monitoring, bijvoorbeeld met cameratoezicht
4. Gevoelige gegevens, zoals bijzondere categorieën van persoonsgegevens (zie artikel 9 van de AVG;
5. Grootschalige gegevensverwerkingen, gezien bv. de hoeveelheid mensen van wie gegevens worden verwerkt, de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt, de tijdsduur van de gegevensverwerking, de geografische reikwijdte van de gegevensverwerking.
6. Gekoppelde databases, zoals databases die voortkomen uit verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.
7. Gegevens over kwetsbare personen, bv. wanneer sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke met als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens.
8. Gebruik van nieuwe technologieën, omdat dit gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.
9. Blokkering van een recht, dienst of contract, waardoor betrokkenen een recht niet kunnen uitoefenen, een dienst niet kunnen gebruiken of een contract niet kunnen afsluiten.

SRK borgt dat bij besluitvorming wordt stilgestaan bij de vraag of een gegevensbeschermingseffectbeoordeling nodig is, door de vraag naar verwerking en risico's in standaard (besluit)documenten op te nemen, evenals in alle (project)plan documenten.

2.7 Privacy by design en privacy by default

Artikel 25 van de AVG is getiteld "Gegevensbescherming door ontwerp en door standaardinstellingen". Kort gezegd schrijft de bepaling voor dat bij het ontwerpen en inrichten van systemen en processen nadrukkelijk met bescherming van persoonsgegevens rekening te houden.

2.7.1. Privacy by design

Door in de ontwerpfase bescherming van persoonsgegevens als criterium te betrekken, wordt het structureel onderdeel van veranderprocessen en ontstaat als vanzelf een hoge graad van bescherming en management van risico's. Dat is in het belang van zowel klanten, ketenpartners, als SRK zelf.

2.7.2. Privacy by default

Door bij standaardinstellingen, -inrichtingen en voorwaarden de bescherming van persoonsgegevens als criterium en standaard te betrekken, worden risico's beperkt en als vanzelf rechten en belangen van betrokkenen gewaarborgd.

SRK geeft vorm en inhoud aan deze verplichtingen, door:

1. bij alle verwerkingen onverminderd als leidend beginsel aan te houden dat functionarissen slechts toegang tot die informatie krijgen, zolang en voor zover dat nodig is bij de uitoefening van hun functie ("need to know"). Dit vormt de basis voor bv. het autorisatieschema.
2. bij alle wijzigingen en vernieuwingen in processen, toepassingen en technieken of technologieën de onderwerpen van *privacy by design* en *privacy by default* in plannen en documenten op te nemen.
3. bij alle wijzigingen en vernieuwingen als bij art 35 lid 1. bedoeld, de FG vooraf te informeren en gelegenheid te geven te adviseren, of actief om advies te vragen als de aard van de wijziging of verwerking daartoe aanleiding geeft.

Hoofdstuk 3 – Beleid inzake Informatiebeveiliging

3.1 Doel van informatiebeveiliging

De primaire en ondersteunende werkzaamheden van SRK zijn sterk afhankelijk van de betrouwbaarheid van informatie, applicaties en een adequate informatievoorziening. Om de informatie en informatievoorziening beheersbaar en betrouwbaar te houden - slechts geautoriseerd op basis van “niet meer dan nodig” - en een behoorlijke en zorgvuldige verwerking te borgen, is het noodzakelijk om een aantal gemeenschappelijke uitgangspunten te bepalen en uit te dragen vanuit vastgesteld beleid.

Het informatiebeveiligingsbeleid is van toepassing op het gehele proces van de informatievoorziening, van zowel geautomatiseerde- als niet geautomatiseerde informatiesystemen, ongeacht de classificatie en opslagwijze.

3.2 Definitie van informatiebeveiliging

Informatiebeveiliging wordt door SRK gedefinieerd als het proces van het beschermen van informatie en daaraan gerelateerde componenten (zoals geautomatiseerde informatiesystemen, personen en papieren documenten) tegen onvoorziene of vooropgezette inbreuken op:

Beschikbaarheid: *De mate waarin informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor geautoriseerde gebruikers.*
Het risico dat de continuïteit van de (kritische) bedrijfsprocessen/de gehele instelling in gevaar komt als gevolg van het niet beschikbaar zijn van de IT-infrastructuur (waaronder applicaties en systemen). Hieronder wordt tevens het risico gezien van het niet toegankelijk zijn van informatie voor geautoriseerde gebruikers.

Integriteit: *De mate waarin de juistheid en volledigheid van informatie en de verwerkingsmethode is gewaarborgd.*
Het risico dat informatie en/of het informatiesysteem niet volledig, juist of accuraat is.

Vertrouwelijkheid: *De mate waarin gewaarborgd wordt dat informatie alleen toegankelijk is voor degenen die hiervoor gerechtigd zijn.*
Hieronder wordt tevens begrepen het risico van het toegankelijk zijn van informatie voor niet geautoriseerde gebruikers.

3.3 Uitgangspunten informatiebeveiligingsbeleid

2.3.1 Integraal risicomanagement

De grondslag voor informatiebeveiliging is risicobeheersing. Informatiebeveiliging wordt vanuit een integrale visie benaderd en waar mogelijk gecombineerd met andere SRK risicomanagementdisciplines (Enterprise Risk Management).

3.3.2 Balans

Maatregelen zijn, als output van een uitgevoerde risicoanalyse, wat inspanning en kosten betreft in balans met het te beschermen belang of waarde (acceptabel risico, acceptabele kosten), in overeenstemming met wet- en regelgeving.

3.3.3 Eigenaarschap

Alle processen, applicaties en generieke infrastructuur (fysiek en informatie) hebben één formele eigenaar in de lijnorganisatie, die vanuit zijn verantwoordelijkheid eisen stelt m.b.t.de beveiliging en te nemen maatregelen t.a.v. de opgeslagen informatie, alsmede de verwerking daarvan, mede door derden. Dit eigenaarschap is belegd bij de betreffende asset owner.

3.3.4 Efficiency

Risico’s worden beperkt tot een aanvaardbaar niveau. Het aanvaardbare niveau wordt vastgesteld en gedocumenteerd door de asset owner. Hierbij worden de (wijzigingen in de) operationele eisen en de financiële randvoorwaarden in overweging genomen. De betrouwbaarheid van een informatiesysteem

dat voorziet in gegevensuitwisseling met derden, moet zijn gewaarborgd, overeenkomstig het belang dat het systeem heeft voor het bedrijfsproces. De ICT afdeling heeft hierbij een faciliterende rol, de asset owner is eindverantwoordelijk

3.3.5 Standaardniveau

SRK hanteert een beschreven standaardniveau van informatiebeveiliging. Dit standaardniveau bestaat uit maatregelen getroffen door onder andere: ICT, Facilities en HRM. Deze maatregelen zijn als basisvoorziening in het pand, zowel fysiek danwel in procedure, aanwezig. Deze standaard dient als een baseline die geldt als minimumniveau.

3.3.6 Beveiligingsbewustzijn

Beveiligingsbewustzijn leidt op ieder niveau binnen de organisatie tot medewerkers die weten voor welke risico's zij verantwoordelijk zijn en hoe en waarom zij de beheersmaatregelen uit moeten voeren. De opzet van het awareness programma wordt opgesteld en uitgevoerd onder verantwoordelijkheid van Legal & Compliance. Het (lijn)management is verantwoordelijk voor de actieve bevordering van informatiebeveiliging t.a.v. de medewerker op de werkplek.

3.3.7 Toegang

Toegang tot informatie wordt toegekend op basis van ‘need-to-know’ ofwel wat moet ik weten om mijn werk goed te kunnen doen. Rechten worden toegekend op basis van ‘need-to-have’ ofwel over welke rechten moet ik beschikken om mijn werk goed te kunnen doen.

3.3.8 Digitale dossiers

Integriteit (de juistheid en volledigheid) van digitale cliëntdossiers/informatie zijn leidend ten opzichte van fysieke cliëntdossiers/informatie.

3.3.9 Classificatie en beheer van bedrijfsmiddelen

Voor alle informatie en applicaties binnen SRK is een eigenaar bekend en vastgelegd. Deze asset owner bepaalt het vereiste classificatieniveau. Dit niveau is in balans met de waarde van de te beschermen informatie. Classificatie van informatie en applicaties vindt plaats op basis van:

- Beschikbaarheid (mate waarin informatie beschikbaar moet zijn)
- Integriteit (mate waarin informatie juist/volledig moet zijn)
- Vertrouwelijkheid (mate waarin informatie openbaar tot bedrijfskritisch is)

Alle bedrijfsmiddelen zijn binnen SRK beveiligd tegen diefstal en schade. Dit niveau is in balans met de waarde van de te beschermen informatie. De afdeling ICT zorgt voor het beheer van de bij SRK toegepaste hard- en software(licenties). Om dit te ondersteunen zijn binnen SRK verschillende processen beschreven conform de beheermethodiek ITIL en BiSL [1]. Deze processen worden jaarlijks geëvalueerd en indien nodig aangepast.

Classificatieniveau Binnen SRK worden 4 classificatieniveaus voor vertrouwelijkheid van informatie gehanteerd, te weten:

- 1. **Geheime informatie** zoals gevoelige informatie over bedrijf(proces) en reorganisaties.
- 2. **Persoonsgegevens** zoals alle gegevens die vallen onder privacy wetgeving.
- 3. **Bedrijfsinformatie** zoals managementinformatie en informatie voor alleen interne communicatie bijvoorbeeld via intranet..
- 4. **Openbaar** zoals informatie op onze website.

In een vastgestelde Standaard Informatie- en Classificatieniveau worden de richtlijnen en omgangseisen voor deze niveaus benoemd. Deze Standaard wordt onderhouden en beheerd door de Information Security Officer, in nauwe samenwerking met de Compliance Officer/Functionaris gegevensbescherming en Informatiemanager.

[1] De Information Technology Infrastructure Library (ITIL) is een gestructureerde aanpak voor het leveren van een gewenste kwaliteit van IT Services. De Business Information Services Library is een framework dat een beschrijving geeft van werkzaamheden die aan de klantzijde moeten worden uitgevoerd in een organisatie om de informatievoorziening te krijgen die zij nodig heeft. We hebben het hier dan meer concreet over functioneel beheer en informatiemanagement.

3.3.10 Afwijkingen op het beleid

Daar waar een bedrijfsonderdeel het voornemen heeft af te wijken van vastgesteld beleid of standaarden, legt het management dit vast in een formele verklaring (comply or explain). De verklaring bevat een vooraf gemaakte risico-inschatting van de afwijking en de mogelijke consequenties en wordt aan de Directie voorgelegd. De Compliance Officer/Functionaris gegevensbescherming heeft hierin een adviserende rol.

3.4 Eisen en maatregelen van informatiebeveiliging

De aan informatiebeveiliging gestelde eisen vloeien voort uit de AVG en uit de eisen die SRK stelt vanuit het oogpunt van continuïteit van de bedrijfsvoering en dienstverlening. Het resultaat is een mate van Beschikbaarheid, Integriteit en Vertrouwelijkheid die past bij de aard van de gegevens en dienstverlening en die onze klanten en ketenpartners, maar ook medewerkers en derden redelijkerwijs van ons mogen verwachten.

Voor de concrete bepaling van deze beveiligingsniveaus en –maatregelen heeft SRK aansluiting gezocht bij het **Toetsingskader Informatiebeveiliging van De Nederlandsche Bank**. Te allen tijde zijn van toepassing de “Control Measures” zoals opgelegd door DNB. Deze zijn beschreven in het DNB Toetsingskader Informatiebeveiliging. Dit kader wordt binnen SRK ook gebruikt om de volwassenheid van informatiebeveiliging periodiek te meten. Dit toetsingskader wordt door toezichthouder DNB sinds 2013 verplicht voorgeschreven binnen de financiële en verzekeraars sector. Door dit model te gebruiken sluit SRK als uitvoeringsorganisatie aan bij rechtsbijstandsverzekeraars als De Goudse, Juwon, de Vereende en andere relevante counterparts. De documenten maken integraal onderdeel uit van het beleid.

3.5 Documentatie

Dit informatiebeveiligingsbeleid is een richtinggevend en strategisch document. De vertaling hiervan in richtlijnen en uitgangspunten wordt weergegeven in tactisch beschreven onderliggende Privacybeschermings- en Informatiebeveiligings(deel)processen. In procedures zijn vervolgens de privacybeschermings-en of IB activiteiten en taken (als werkinstructie) meer gedetailleerd en concreet beschreven. Alle relevante documentatie wordt namens de verantwoordelijke Directeur Financiën & ICT beheerd door de Information Security Officer.

3.6 Processen/procedures

Uit het informatiebeveiligingsbeleid volgen een aantal specifieke processen/procedures over de volgende onderwerpen. De inhoud hiervan wordt gepubliceerd op Intranet.

3.6.1 Informatiebeveiligingseisen bij uitbesteding

3.6.2 Toegangsrechten

3.6.3 Omgang mobile gegevensdragers

3.6.4 Business Continuity plan

3.6.5 IB Incidenten beheer

3.6.6 Fysieke beveiliging

3.7 Bedrijfsonderdelen met ondersteunende taken

Bedrijfsonderdelen met SRK-brede generieke ondersteunende taken hebben, naast het beschermen van de eigen informatie, een aanvullende verantwoordelijkheid met betrekking tot de levering van generieke beveiligingsdiensten aan andere bedrijfsonderdelen.

Facilities:	Levert fysieke toegangsbeveiliging en technisch bouwkundige (brand)beveiliging.
ICT:	Levert veilige IT-infrastructuur.
HRM:	Toetst de betrouwbaarheid van intern en extern personeel / levert integriteitstoetsing van medewerkers.

3.8 Risicomanagement

De grondslag voor informatiebeveiliging is risicobeheersing. Informatiebeveiliging wordt vanuit een integrale visie benaderd en is een onderdeel van het SRK Enterprise Risk Managementproces.

De omvang van het informatiebeveiligingsrisico en het risico op een inbreuk op de privacy van betrokkenen wordt bepaald door het karakter van SRK als rechtshulpverlener, dat inherent veelvoudig informatie/persoonsgegevens verwerkt. SRK stelt jaarlijks een overzicht samen waarin de risico matrix van (kritische) bedrijfsprocessen en hun ondersteunende informatiesystemen duidelijk wordt weergegeven. Voor de risico's met betrekking tot schending van de privacy voert SRK continu de registratie van verwerkingsactiviteiten welk register input levert voor de risico analyse ter zake een inbreuk op de privacy van betrokkenen. Tijdens deze analyses wordt geïnventariseerd welke risico's zich kunnen voordoen en kijkt men vooruit (preventie). De risicoanalyse wordt op periodieke basis uitgevoerd. Dit leidt tot een gemeenschappelijk gedragen risicoprofiel waarin risico's op basis van impact, waarschijnlijkheid en control effectiviteit in samenhang zijn beoordeeld.

Ten aanzien van risico's die voort komen uit de risicoanalyse zal SRK per risico steeds één van de volgende strategieën kiezen om deze te verkleinen:

- Treat the risk (reduceren): verkleinen van het risico door middel van het nemen van informatiebeveiligingsmaatregelen.
- Take the risk (accepteren): het risico is zo klein dat de gevolgen acceptabel zijn.
- Terminate the risk (vermijden): wanneer een er een groot risico bestaat voor een bedrijfsactiviteit die weinig tot niets oplevert dan wordt deze bedrijfsactiviteit gestaakt.
- Transfer the risk (delen/overdragen): overhevelen van het risico naar een derde partij door middel van uitbesteding of het afsluiten van verzekeringen.

Hoofdstuk 4 - Governance en bestuurlijke kaders

4.1 Bestuurlijk kader

Binnen SRK is de organisatorische structuur voor informatiebeveiliging- en privacybescherming als volgt:

De Directie van SRK is eindverantwoordelijk voor het laten opstellen, onderhouden en naleving van het informatiebeveiligings- en privacybeschermingsbeleid en het incorperen van het beleid in de dagelijkse processen. De Directeur Financiën & ICT is hiervoor als portefeuillehouder aangewezen en laat zich daarbij adviseren door de Functionaris voor gegevensbescherming en de Information security officer.

Het (lijn)management is verantwoordelijk voor de uitvoering van het informatiebeveiligings- en privacybescherming beleid op de werkvloer. Het vergroten van awareness is hierin een belangrijke taak.

De functionaris voor gegevensbescherming en de Information security officer zijn in samenspraak verantwoordelijk voor het bewaken van opzet, bestaan en werking van privacybescherming en informatiebeveiliging, in relatie tot geldende wet- en regelgeving.

De Contractmanager ziet toe op verwerking van de eisen van SRK in samenwerkingsrelaties en contractuele voorwaarden, waaronder de verwerkersovereenkomst, privacy by design en default.

Iedere medewerker is verantwoordelijk en aansprakelijk voor de beveiliging van de informatie (waaronder persoonsgegevens) die hem of haar zijn toevertrouwd.

De Stuurgroep Informatiebeveiliging en Privacybescherming bestaat uit de Directeur Financiën & ICT (voorzitter), de Information Security Officer, de Compliance Officer tevens Functionaris voor gegevensbescherming. De Stuurgroep adviseert de Directie over de inrichting van Privacybescherming en Information Security Management Systeem (ISMS) en de hieruit voortvloeiende jaarlijkse planvorming, en rapporteert over de voortgang ervan.

In de onderstaande tabel 1 worden de taken, bevoegdheden en verantwoordelijkheden weergegeven:

Functie	*Strategisch (uitstippelen)*	*Tactisch (aansturing)*	*Operationeel (uitvoering)*
Directie	Goedkeuren en uitdragen informatiebeveiligings- en privacybeschermingsbeleid beleid Samenhang met overige beleidsvoornemens en meer jaren planning bewaken	Met ondersteuning van de functies van FG en ISO toezicht houden op informatiebeveiliging en privacybescherming	Naleven van informatiebeveiligings-maatregelen. Voorbeeldfunctie
Directeur Financiën & ICT	Informatiebeveiliging- en privacy risico's regelmatig (laten) actualiseren Beschikbaar stellen middelen voor implementatie van maatregelen inzake informatiebeveiliging en privacybescherming Reviewen van opgeleverd beleid, beleidsvoornemens, planvorming, audit resultaten en overige rapportages; Informeren van de auditcommissie RvC	Voorzitten van de Stuurgroep informatiebeveiliging privacybescherming	Naleven van informatiebeveiligings-maatregelen Bewaken voortgang Voorzitter van Stuurgroep Informatiebeveiliging
Compliance Officer/FG	Verifiëren van en adviseren over het Informatiebeveiligings-privacybeschermingsbeleid Bewaken contractuele verhoudingen	Initiëren van interne en externe audits. Borgen en toegankelijk maken van kennis van de AVG en relevante regelgeving Vertaling van de eisen in bepalingen van de (verwerkings) overeenkomst	Adviseren en rapporteren over compliance component van Informatiebeveiliging Deelnemen aan Stuurgroep Informatiebeveiliging Afwikkeling IB en privacy incidenten

			Voorbereiden en assisteren bij contracteren
Manager ICT (in rol van ISO)	Coördineren informatiebeveiliging Opstellen informatiebeveiligingsbeleid Opstellen periodiek informatiebeveiligingsplan	Uitvoeren en coördineren van risicoanalyses op proces en informatiesystemen Uitvoeren en coördineren van selfassesments informatiebeveiliging (doen) uitvoeren van audits bij verwerkers op basis van verwerkersovereenkomst Coördineren bewustwordingsproces Opzetten en onderhouden van awareness IB en privacybescherming	Naleven van informatiebeveiligings-maatregelen Bewaken voortgang Rapporteren status informatiebeveiliging Deelnemen aan Stuurgroep Informatiebeveiliging Voorzitter werkgroep awareness
Lijnmanagement	Bepalen van BIV rating van applicaties (asset-owner)	Bijdragen aan risicoanalyse informatiebeveiliging voor proces en informatiesystemen Implementeren specifieke informatiebeveiligingsmaatregelen voor eigen afdeling Bevorderen bewustwording eigen medewerkers Toezicht houden op naleving van informatiebeveiliging maatregelen door zijn/haar medewerkers.	Controleren correctheid inhoud functie rollen (RBAC)
Informatie Manager	Verantwoordelijk voor het verwerkingenregister als instrument en de organisatie van actueel en volledig houden	Periodieke evaluaties, aanvullen en onderhouden i.o.m. management	Zorgen voor input, onderhoud en naleving Actueel houden van rubricering informatietypen en classificatie
Medewerkers	n.v.t.	Instandhouden van een professionele cultuur	Naleven van beveiligingsmaatregelen. Naleven van de eisen die aan de rechtshulpverlener worden gesteld i.v.m. vertrouwelijkheid

Hoofdstuk 5 – Beleidscyclus

5.1 Beleidscyclus

Binnen SRK is een Information Security management proces (ISMS) ingericht conform de norm ISO27001. Deze cyclus is gericht op het voldoen aan in- en externe beveiligingseisen en het realiseren van een zeker basisniveau aan beveiliging. SRK zal het proces hiertoe vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren. Het belang van privacy bescherming volgt dezelfde beleidscyclus als het ISMS

- Binnen SRK wordt conform het onderstaande beheerkader in een managementcyclus de implementatie van privacybescherming en informatiebeveiliging in de organisatie geïnitieerd en beheerst.
- Het privacybescherming en informatiebeveiligingsbeleid wordt door de Directie van SRK goedgekeurd, rollen worden toegewezen en de implementatie van de maatregelen binnen SRK wordt door de respectievelijke Managers gecoördineerd en beoordeeld.
- Omdat het primaire proces en de ondersteunende IT-voorzieningen continu onderhevig zijn aan veranderingen, is privacybescherming en Informatiebeveiliging binnen SRK een continu (verbeter)proces.
- Het privacybescherming- en informatiebeveiligingsproces doorloopt de zogenaamde Deming Cyclus die de fases Plan, Do, Check en Act bevat.

5.2 Beoordeling en evaluatie

Beoordeling
Het privacybeschermings- en informatiebeveiligingsbeleid (en het daaraan gekoppelde plan en processen) wordt jaarlijks beoordeeld op de opzet, bestaan en werking. Informatiebeveiliging kan ook deel uitmaken van de jaarlijkse externe accountantscontrole.

Evaluatie
Nadat beoordeling van het privacybeschermings- en informatiebeveiligingsbeleid, plan en processen jaarlijks heeft plaatsgevonden worden bevindingen in een rapportage aangeboden aan de Directie. Afhankelijk van de bevindingen leiden deze tot verbetervoorstellen. Op deze manier wordt vorm gegeven aan een constante aandacht door middel van de Deming cirkel (Do-Plan-Check-Act), zodat een frequente toetsing en waar noodzakelijk aanpassing, van het bestaande beleid zal plaatsvinden.