**Beleidskader**

Aan: <besluitvormend orgaan>

Van: <auteur(s)>

Betreft: beleidskader gegevensbescherming

Datum: <datum>

Kenmerk: <kenmerk>

Het beleidskader inzake gegevensbescherming (hierna te noemen BKGB) van <naam voluit als bedoeld in de statuten> (hierna te noemen <naam organisatie in het dagelijks gebruik>) bevat de afspraken tussen het bestuur en organisatie. Deze afspraken moeten worden nagekomen in alle gevallen dat bedrijfsgegevens, inclusief persoonsgegevens, worden gebruikt, opgeslagen of uitgewisseld (‘verwerking van gegevens’).

1. **Doel**

Het doel van het BKGB is om te waarborgen dat uw organisatie de wet- en regelgeving, richtlijnen en normen in de zorgsector en afspraken in overeenkomsten naleeft, zodat er sprake is van een behoorlijke- en zorgvuldige verwerking en beheer van gegevens.

1. **Visie en missie**

Uw organisatie ziet de bescherming van gegevens als een zaak van behoorlijk bestuur. In de maatschappij moeten burgers, personeel, externen, bestuur, leveranciers en ledenorganisaties, en hun contactpersonen, erop vertrouwen dat we hun gegevens op rechtmatig, zorgvuldig en veilig verwerken. Wie voor ons werkt, begrijpt dit en laat zich hierdoor leiden in zijn of haar werk binnen en voor Uw organisatie. Het bestuur van uw organisatie schept de voorwaarden voor een gegevensbewuste organisatiecultuur en voert in dat kader niet aflatend gegevensbeschermingsbeleid. We zijn transparant over onze gegevensverwerking en de manier waarop wij gegevens beschermen. Bij dilemma’s gaan wij de dialoog aan met betrokkenen en zoeken gezamenlijk naar oplossingen.

1. **Kernpunten**
2. Zorg voor data is een bestuurlijke verantwoordelijkheid. Het bestuur en de proceseigenaren sturen op gegevensbescherming volgens deze kernpunten van gegevensmanagement:
	1. Een proceseigenaar voert, als onderdeel van zijn verantwoordelijkheid, regie en houdt toezicht op zijn proces(sen) op basis van dit BKGB.
	2. Bij processen waaraan risico’s zijn verbonden, als het gaat om bescherming van data en/of privacy, hanteert de proceseigenaar een procesplan.
	3. Een procesplan is duidelijk, actueel, stemt overeen met de werkelijkheid en wordt periodiek geëvalueerd.
	4. Binnen een proces worden gegevens alleen verwerkt voor het realiseren van het procesdoel.
	5. Binnen een proces worden geen onrechtmatig verkregen gegevens verwerkt.
	6. Een procesplan benoemt de waarborgen voor eerlijke, veilige en betrouwbare procesvoering.
	7. Een procesplan omvat eventuele opdrachten aan de organisatie en afspraken over toezicht door de proceseigenaar op goede uitvoering van werkzaamheden.
	8. Een proceseigenaar handelt vragen of klachten van derden of medewerkers binnen twee weken af.
	9. Bij incidenten hanteert de proceseigenaar de Werkinstructie inzake melden van incidenten.
	10. Bij risicovolle procesvoering laat de proceseigenaar zich periodiek auditen op grond van dit BKGB en de desbetreffende procesplan.
3. Het bestuur voorziet in een professional op het gebied van gegevensbescherming die het bestuur en de proceseigenaren ondersteunt in de beleidsuitvoering.
4. Het bestuur voorziet zichzelf en de organisatie in faciliteiten voor bewustwording en training.
5. Uw organisatie beschikt over mechanismes voor incidentmanagement.
6. Uw organisatie evalueert per twee jaar de doeltreffendheid en de doelmatigheid van het BKGB.
7. Het bestuur informeert de stakeholders over de beleidsuitvoering inzake gegevens-bescherming.
8. Het bestuur handhaaft het beleid en heeft een verantwoordelijke aangesteld, die toeziet op de naleving van het BKGB enerzijds en wet- en regelgeving anderzijds.
9. **Scope**

Het BKGB van uw organisatie is van toepassing op de gehele bedrijfsvoering van deze vereniging en daarover zeggenschap heeft.

Het BKGB is het algemene deel van het gegevensbeschermingsbeleid binnen uw organisatie. Het algemene beleidskader is de kapstok voor dat beleid, waaraan aanvullende regelingen worden opgehangen, zoals procesplannen of regelingen voor het uitoefenen van rechten, codes en autorisaties.

Het beleid:

* omvat zowel bedrijfsprocessen als de onderliggende voorzieningen voor informatieverwerking en gegevensopslag. Papieren of digitale informatieverwerking maakt geen verschil;
* is van toepassing op processen die uw organisatie uitbesteedt, inkoopt of op een andere manier organiseert, zoals deelname in een rechtspersoon die voor uw organisatie diensten verricht;
* omvat de gehele ‘data life cycle’: van genereren of verzamelen van gegevens, het gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging;
* is van toepassing op de verwerking van statistieken en/of (geanonimiseerde) gegevens, voor zover niet kan worden uitgesloten dat natuurlijke personen kunnen worden geïdentificeerd of geprofileerd;
* is van toepassing op informatie-veiligheidsproblemen.
1. **Raakvlakken**

Het gegevensbeschermingsbeleid van uw organisatie heeft raakvlakken met andere beleidsthema’s of vertoont hiermee overlap.

Integriteitsbeleid

Beleidsuitvoering is gekoppeld aan de beginselen van behoorlijk bestuur en is daarmee ondersteunend aan het integriteitsbeleid binnen en het bestuur en binnen de organisatie.

Kwaliteitsbeleid

Beleid richt zich in belangrijke mate op het waarborgen van een kwalitatief goede administratieve organisatie. Een kwalitatief goede administratieve organisatie is randvoorwaardelijk voor klantgerichte- en klantvriendelijke taakuitoefening (‘de mens centraal’).

Continuïteit en risicomanagement

Beleid schept waarborgen op het gebied van continuïteit en risicomanagement, omdat gegevensbeschermingsbeleid afbreuk- en aansprakelijkheidsrisico’s tegengaat en voorkomt dat werkprocessen spaak lopen, daar de bijbehorende gegevensverwerking een schending van rechten en plichten inhouden (‘onrechtmatige daad’).

Informatiebeveiliging

Beleid ondersteunt het informatiebeveiligingsbeleid door de nadrukkelijke aandacht voor het tegengaan van incidenten die de beschikbaarheid, integriteit en vertrouwelijkheid aantasten van de informatievoorziening en opgeslagen gegevens noch dat deze gegevens (op welke wijze dan ook) worden afgetapt of afgeluisterd. Informatiebeveiliging wordt uitgevoerd op basis van informatiebeveiligingsbeleid.

Communicatie

Het sturen op doelgroepgerichte communicatie wordt gedaan vanuit het communicatiebeleid.

1. **Gegevensbeschermingsmanagement**

Het bestuur is verantwoordelijk voor de naleving van het BKGB en van de wet- en regelgeving, richtlijnen en normen binnen de zorgsector, en voert proactief gegevensbeschermingsbeleid op basis van afweging van belangen en risico’s bij de verwerking van gegevens, zodat dit evenwichtig plaatsvindt. Dat wil zeggen, behoorlijk, zorgvuldig en in overeenstemming met het BKGB, de wet- en regelgeving en conform richtlijnen en normen binnen de zorgsector.

Gegevensbeschermingsmanagement is SMART-georganiseerd en heeft de aandacht van het bestuur. Het bestuur legt over de beleidsuitvoering verantwoording af aan stakeholders en betracht beleidstransparantie met behulp van publieksvoorlichting.

Het bestuur draagt zorg voor de documentatie van beleid en maatregelen, zodat het op ieder moment maatschappelijk- en juridisch uitleg kan geven over de deugdelijkheid van de aanpak. Het bestuur houdt een register van de gegevensverwerkingen bij, die onder zijn verantwoordelijkheid plaatsvinden.

1. **Managementstructuur**

Het bestuur is verantwoordelijk en daarmee voor het voorzien van passende waarborgen bij de uitvoering van de taken binnen de organisatie van deze vereniging.

Gegevensbescherming valt onder de verantwoordelijkheid van dat bestuur. Immers, governance en compliance is een belangrijk aandachtspunt voor het dagelijks bestuur.

Het bestuur kan op grond van de AVG een Functionaris gegevensbescherming (FG) benoemen. De FG adviseert het bestuur, gevraagd en ongevraagd.

1. **Eigenaarschap**

De leden van het managementteam (MT) zijn ervoor verantwoordelijk dat de taakuitoefening, waarvoor een productgroep verantwoordelijk is, binnen de grenzen van dit BKGB plaatsvindt en rapporteren over dit laatste aan het bestuur.

Daarmee is een MT-lid de proceseigenaar. Dat lid kan deze rol niet door-mandateren naar anderen binnen de organisatie. Het bestuur blijft eindverantwoordelijk voor de bestendigheid van de processen binnen de organisatie als verwerkings-verantwoordelijke.

Proceseigenaren voeren regie over de proces(sen) binnen hun groep(en) op basis van procesplannen, die voldoende overzicht bieden van de procesvoering voor effectieve sturing. Een procesplan dient te passen binnen dit BKGB en is steeds in overeenstemming met de feitelijke situatie. Veranderd deze situatie, dan wordt het procesplan direct geactualiseerd.

Een proceseigenaar houdt proactief toezicht op de databestendigheid van de organisatie van het proces in zijn groep(en) en documenteert keuzes en oplossingen als bijlagen van het procesplan en informeert de bestuurder hierover direct. Immers, het bestuur zal wel eerst hiermee akkoord moeten gaan.

1. **Toezicht**

De FG is de interne toezichthouder op de naleving van BKGB en wet- en regelgeving. Onder bepaalde omstandigheden is deze verplicht binnen een organisatie, in andere gevallen worden organisatie gestimuleerd dit vrijwillig te doen. Het bestuur van uw organisatie moet hieraan gehoor door zonder meer een FG aan te stellen.

Het bestuur wijst een natuurlijk persoon aan als FG en informeert in- en externe doelgroepen daarover en worden de contactgegevens van deze ene FG onder de aandacht gebracht van de Autoriteit Persoonsgegevens (AP).

De FG wordt aangewezen op grond van:

* zijn professionele kwaliteiten en in het bijzonder, zijn deskundigheid op het gebied van wet- en regelgeving, richtlijnen en normen, en de gegevensbescherming managementpraktijk en;
* zijn vermogen om de onderstaande taken te vervullen.

De FG:

* informeert en adviseert het bestuur en proceseigenaren over de werking van het beleid van de Uw organisatie en nakoming van achterliggende verplichtingen (en heeft de lead in interpretatie van wet- en regelgeving en aangegane verplichtingen met derden);
* houdt toezicht op de nakoming van het beleid en achterliggende wettelijke verplichtingen;
* helpt klachten tot een goed einde te brengen (ombudsfunctie);
* adviseert bij incidenten over ernst en omvang;
* beheert het BKGB van Uw organisatie;
* ziet toe op het beheer door het bestuur van het register van verwerkingen;
* controleert de naleving van afspraken door Uw organisatie en partners;
* helpt het beleid uit te dragen bij interne- en externe doelgroepen.

De FG krijgt de nodige ruimte voor professionele uitvoering van taken. Namelijk:

* het bestuur en proceseigenaren zorgen ervoor dat de FG naar behoren en tijdig wordt betrokken bij de verwerking van gegevens;
* de FG wordt volledig geïnformeerd over aspecten van de bedrijfsvoering binnen Uw organisatie, waarbij gegevens worden verwerkt of wanneer daartoe voornemens bestaan;
* het bestuur en proceseigenaren ondersteunen de FG door op zijn verzoek toegang te geven tot de verwerking van gegevens en hem de middelen te bieden voor professioneel onderzoek.

De zienswijze van de FG is zwaarwegend en geldt als richtinggevend voor naleving van het gegevensbeschermingsbeleid binnen uw organisatie.

De FG doet jaarlijks verslag van zijn werkzaamheden aan het bestuur. Het bestuur voegt dit toe aan haar jaarverslag. Op deze wijze verantwoord het bestuur zich richting alle stakeholders en met name richting betrokkenen die gebruik hebben gemaakt van de diensten van Uw organisatie. Belangrijk is, dat zij het gevoel hebben dat deze organisatie zorgvuldig omgaat met hun gegevens en hierdoor veilig kan bezoeken en gebruik kunnen maken van deze diensten.

1. **Gegevensverwerking**

Uw organisatie is zich bewust van de maatschappelijke verantwoordelijkheid die gepaard gaat met de verwerking van gegevens in het algemeen en die van natuurlijke personen in het bijzonder. Om deze reden:

* voert uw organisatie proactief beleid op basis van dit BKGB;
* faciliteert uw organisatie de uitoefening van rechten van (rechts-) personen;
* bewaakt uw organisatie de goede nakoming van wet- en regelgeving.

Noodzakelijkheid

Proceseigenaren verwerken gegevens uitsluitend voor de volgende doelen, voor zover dit valt binnen hun mandaat en noodzakelijk is voor:

* de uitoefening van de taken;
* de nakoming van wettelijke- en juridische verplichtingen;
* de vrijwaring van vitale belangen voor betrokkene(n);
* de totstandkoming of uitvoering van een overeenkomst, waarbij betrokkene partij is;
* de behartiging van een gerechtvaardigd belang van uw organisatie of een derde aan wie gegevens worden verstrekt, tenzij het recht op de bescherming van de persoonlijke levenssfeer of bedrijfsgeheim prevaleert.

Kapstokregeling

Het BKGB van Uw organisatie heeft een algemeen karakter en een raamwerkfunctie (kapstokregeling). Het zoomt niet in op de spelregels die kunnen gelden voor specifieke activiteiten. Voor zover dit speelt, geven proceseigenaren via themabeleid en procesplannen nadere invulling aan het BKGB van Uw organisatie, in samen-spraak met de FG.

Procesplannen en beschrijving van werkprocessen, de bijbehorende gegevens-verwerking en de waarborgen waarmee de werkprocessen omkleed zijn, zodat een databestendige aanpak ontstaat. Dat wordt versterkt door daaraan een beveiligings-plan toe te voegen, waarin is opgenomen welke waarborgen er zijn om incidenten te voorkomen of althans de kans daarop zo minimaal mogelijke te houden, zowel in het algemeen bij alle bedrijfsgegevens en in het bijzonder bij persoonsgegevens en zeer specifiek bij bijzondere persoonsgegevens.

Het BKGB van uw organisatie bevat ook de aanzet voor het regelen van aspecten van beleidsvoering die onder de directe verantwoordelijkheid van het bestuur vallen.

Het BKGB van uw organisatie, themabeleid, procesplannen, veiligheidsplan en de daadwerkelijke uitvoering hiervan via organisatorische-, technische- en juridische oplossingen, vormen samen het beleid van uw organisatie.

Bijzondere voorschriften

Op basis van het BKGB van Uw organisatie geeft deze organisatie uitvoering aan wet- en regelgeving. Voor zover van toepassing, houdt het bestuur tevens goed rekening met bijzondere wettelijke voorschriften.

1. **Gedragsnorm**

Het bestuur verwacht van proceseigenaren rechtmatige- en zorgvuldige verwerking van gegevens. Proceseigenaren kunnen hiervoor rekenen op support door de FG. Het bestuur voert ook op andere manieren voorwaardenscheppend beleid teneinde binnen uw organisatie een gegevensbestendige cultuur te realiseren.

Proceseigenaren voorzien in passende organisatorische- en technische oplossingen om de rechtmatigheid, proportionaliteit, juistheid, veiligheid van gegevensverwerking te waarborgen (‘data-waarborgen’) en documenteren die maatregelen in proces-plannen.

Het bestuur of namens het bestuur houdt de organisatie een register bij van de gegevensverwerkingen die onder de eindverantwoordelijkheid van het bestuur vallen. Proceseigenaren helpen om dat register volledig en actueel te laten zijn (door middel van een formulier).

Het bestuur is transparant over de bedrijfsvoering, gegevensverwerking en beleidsuitvoering en faciliteert de uitoefening van de rechten door (rechts-) personen over wie Uw organisatie gegevens verwerkt (‘doelmatigheid’). Proceseigenaren verlenen hieraan hun medewerking.

Het bestuur en proceseigenaren dragen het belang uit van de beleidsuitvoering en geven zelf het goede voorbeeld. Zij maken gegevensbescherming bespreekbaar. Bij dilemma’s gaan zij de dialoog aan met doelgroepen over wie informatie wordt verwerkt.

Aanpak

Aan procesplannen liggen assessments ten grondslag. Assessments zijn instrumenteel voor het kunnen bepalen van passende beheersmaatregelen. De mate waarin en de manier waarop bedrijfsprocessen en gegevensverwerking aandacht nodig hebben, hangen samen met de uitkomsten van het assessment, zoals verwoord in het assessmentrapport. Een systematiek voor het onderzoek en vastlegging in een rapport wordt nader bepaald. Assessmentrapporten worden opgesteld conform artikel 35, lid 7, AVG, als het gaat om persoonsgegevens. Het bestuur is hiervoor verantwoordelijk.

Proceseigenaren documenteren met behulp van hun procesplannen hoe zij op een praktische manier in passende organisatorische- en technische gegevens-beschermende maatregelen voorzien, met name om de volgende fouten te voorkomen:

* illegale/onrechtmatige gegevensverwerking: gebruik, opslag of uitwisseling van informatie is verboden (middels een rechtstreeks verbod of een beperking van het toegestane gebruik);
* disproportionele gegevensverwerking: gebruik, opslag en uitwisseling van informatie is:
	+ ontoereikend of juist overmatig;
	+ het organisatiebelang bij de gegevensverwerking is onevenredig klein, terwijl de impact op (rechts-) personen onevenredig nadelig kan zijn;
* irrelevante gegevensverwerking: de gebruikte, opgeslagen of uitgewisselde informatie dient geen bedrijfsdoel, doet niet ter zake of is verouderd;
* onnauwkeurige gegevensverwerking: de gebruikte, opgeslagen of uitgewisselde informatie is geen juiste weergave van de werkelijkheid;
* onveilige gegevensverwerking: de gebruikte, opgeslagen of uitgewisselde informatie dreigt gemakkelijk toegankelijk te zijn voor onbevoegden, gemanipuleerd te worden of onbeschikbaar te raken;
* niet-inachtneming van bijzondere wettelijke voorschriften: de gebruikte, opgeslagen of uitgewisselde informatie worden formele verplichtingen veronachtzaamd;
* onbewaakte gegevensverwerking: de proceseigenaar verzuimt om te controleren of de waarborgende maatregelen daadwerkelijk zijn geëffectueerd of te evalueren in hoeverre zijn procesplan bijstelling behoeft.

Key controles

Proceseigenaren vatten, in samenspraak met het bestuur en zo nodig de FG, hun procesplannen samen in een lijst van kenmerkende beheersmaatregelen (´key controles´) voor sturingsdoeleinden en controle. Daartoe wordt nader een systematiek ontwikkeld. Proceseigenaren nemen de lijst van key controles op aan het einde van het procesplan.

FG-verklaring

Een evenwichtig procesplan beschrijft een behoorlijke- en zorgvuldige aanpak, in overeenstemming met de BKGB en de wet. De FG bevestigt dit aan de hand van een verklaring, waarbij hij eventueel ook aanbevelingen doet voor verdere optimalisering van de bedrijfsvoering vanuit het oogpunt van gegevensbescherming. De proceseigenaren nemen FG-verklaringen op aan het einde van het procesplan.

Formulieren

Proceseigenaren vatten hun procesplan samen in een zogenaamde ‘artikel-30-formulier’ dat zij opnemen aan het begin van het procesplan en waarvan zij een afschrift verstrekken aan het bestuur voor opname in het zogenaamde ‘artikel-30-register’. Proceseigenaren melden veranderingen voor dat register onmiddellijk aan de hand van een wijzigingsformulier. Voor deze formulieren komt een nadere opzet beschikbaar.

Primair is dit register bestemd voor registratie van persoonsgegevens, maar in het kader van het BKGB gaat het om alle data. Hierdoor kan dit register ook worden aangewend om na te gaan of er synergie mogelijk is bij de gegevensverwerkingen en doelmatigheid bevorderd kan worden enerzijds en een hulpmiddel voor data-analyse (‘big data en analytics’) anderzijds.

Beheer procesplan

De proceseigenaar is verantwoordelijk voor het beheer van zijn procesplan. Een procesplan wordt bijgesteld wanneer in de praktijk blijkt dat de maatregelen onvoldoende passend blijken naar aanleiding van terechte klachten of (onacceptabele) incidenten. Hoe dan ook evalueert de proceseigenaar een procesplan periodiek en vraagt zo nodig de FG om hierbij advies uit te brengen. De proceseigenaar evalueert dit niet alleen, dit doet hij samen met de desbetreffende productgroep en het bestuur. Welke termijnen van toepassing zijn bij deze periodieke evaluaties wordt nader vastgesteld.

1. **Services**

(Rechts-) personen hebben rechten, mogen vragen stellen en klachten indienen, maar ook in beroep gaan. Daarbij is Uw organisatie faciliterend. De services van deze vereniging is ook daarop ingesteld.

Rechten

(Rechts-) personen hebben er onder andere recht op, dat:

* uw organisatie handelt conform het BKGB;
* uw organisatie niet de contactgegevens van de FG bekend maakt;
* uw organisatie informatie verschaft over doelen van informatieverwerking en gegevensbeleidsuitvoering;
* zij inzage hebben in hun eigen gegevens;
* zij – in geval van fouten – hun gegevens kunnen (laten) rectificeren of verwijderen;
* om tegen het gebruik van hun gegevens verzet aan te tekenen, wat het bestuur verplicht tot het maken van een afweging;
* zij de vereniging bij niet-naleving van het BKGB van Uw organisatie (of de wet) hierop mogen aanspreken.

Vragen

Bij vragen:

* hebben (rechts-) personen het recht om zich te wenden tot de proces-eigenaar;
* vragen worden genoteerd en zo snel mogelijk (of indien mogelijk direct), maar uiterlijk binnen vier weken afgehandeld;
* de proceseigenaar kan de desbetreffende productgroep om advies over de beantwoording vragen;
* een niet tot tevredenheid afgehandelde vraag geeft het recht om zich opnieuw te wenden tot de proceseigenaar. De proceseigenaar registreert in dat geval de vraag als een klacht.

Klacht

Bij klachten:

* hebben (rechts-) personen het recht om zicht te wenden tot het bestuur;
* klachten worden zo snel mogelijk, maar uiterlijk binnen twee weken afgehandeld;
* het bestuur betrekt de desbetreffende productgroep bij de feitelijke klachten-afhandeling;
* het bestuur onderzoekt de gegrondheid van de klacht, waarbij zij nagaat of de klacht betrekking heeft op de naleving van wet- en regelgeving en/of gegevensbeschermingsbeleid van uw organisatie;
* de productgroep kan de GV om advies vragen over de afhandeling van de klacht.

Beroep

(Rechts-) personen hebben het recht om na afhandeling van een klacht, hiertegen in beroep te gaan bij de AP voor zover het beroep gericht is op de naleving van privacywet- en regelgeving.

1. **Programma**

Het bestuur stelt jaarlijks een werkprogramma vast, mede op basis van de jaarrapportage van de FG en de aanbevelingen die hij hierin doet. Het werkprogramma bevordert opzet, bestaan en werking van passende waarborgen voor de bescherming van gegevens binnen de kaders van het BKGB van uw organisatie, mede in het licht van wet- en regelgeving, aanpassing richtlijnen en normen in het werkveld. Dat werkprogramma is met name gericht op het realiseren en in stand houden van een gegevensbestendige bedrijfscultuur binnen uw organisatie, met gebruikmaking van overige instrumenten die hierna worden genoemd.

Bewustwording

Het bestuur bevordert samen met de proceseigenaren een gegevensbewuste organisatiecultuur via voorbeeldgedrag en door te voorzien in de middelen voor bewustwording en, zo nodig, training van alle medewerkers.

Communicatie

Het bestuur is transparant over de gegevensbeschermingsbeleidsuitvoering en voert op dit thema evenwichtig communicatiebeleid, waarbij proceseigenaren zo nodig voorzien zijn in bijzondere voorlichting aan specifieke doelgroepen.

Beheer

Het bestuur voorziet samen met de proceseigenaren in met passende waarborgen omklede verdere verwerking van gegevens voor verenigbare doelen, zoals het genereren van bestuursinformatie. Ook wordt voorzien in passende waarborgen omklede oplossingen voor archivering en adequate waarborgen omklede oplossingen voor archivering en adequate oplossingen voor gegevensvernietiging.

Informatiebeveiliging

Het bestuur ziet erop toe dat informatieveiligheid van uw organisatie in lijn met de geldende norm wordt georganiseerd. Daarbij werkt het bestuur samen met de systeembeheerder tevens coördinator informatiebeveiliger enerzijds en de functioneel-beheerders anderzijds.

Geheimhoudingsverklaringen, Concurrentiebeding en Verklaringen Omtrent Gedrag (VOG) zijn instrumenten binnen de aanpak van uw organisatie voor gegevensbescherming en informatieveiligheid. Bij bepaalde processen kunnen aanvullende geheimhoudingsafspraken worden gehanteerd voor zover uit assessment blijkt dat extra waarborgen op het gebied van vertrouwelijkheid/geheimhouding functioneel zijn.

Incidenten

Het bestuur voorziet in een procedure voor incidenten. Deze procedure bevat in ieder geval een meldplicht voor gebeurtenissen die de beschikbaarheid, integriteit, geheimhouding en vertrouwelijkheid van en bij de informatievoorzieningen en gegevensopslag aantasten, inclusief het vermoeden op afluisteren en aftappen. Ook bevordert het bestuur het oefenen op incidenten, incidentmanagement en crisiscommunicatie.

Handhaving

Het bestuur handhaaft het gegevensbeschermingsbeleid van uw organisatie op basis van een regeling voor waardering van voorbeeldig gedrag en disciplinaire maatregelen bij niet-nakomen van afspraken volgens het BKGB.

Evaluatie

De proceseigenaren doen jaarlijks verslag (verantwoording) aan het bestuur over het gegevensbeschermingsbeleid, oplossingen en incidenten die onder zijn verantwoordelijkheid hebben voorgedaan met een afschrift aan de FG.

De FG doet jaarlijks verslag (beschouwend) aan het bestuur en geeft desgewenst aanbevelingen die strekken tot verdere optimalisering van de gegevensbeschermingsbeleidsvoering. Het bestuur besluit over bijsturing van dat beleid van uw organisatie met inachtneming van de aanbevelingen van de FG.