Stichting De Samenwerking
Pensioenfonds voor het
Slagersbedrijf

Privacybeleid

Titel : Privacy beleid
Datum : 5 april 2018
Referentie : 1804-0329 v0.1
Project : 2018-0421 Vergadering Pensioenfonds Slagers Bestuur (+RvT) 10 april 2018

Inhoud

Algemeen

Dit beleid beschrijft de wijze waarop de privacy beschermd wordt bij de verwerking van persoonsgegevens binnen het pensioenfonds voor het Slagersbedrijf (BPS). BPS hecht er veel waarde aan dat iedere natuurlijke persoon erop vertrouwen kan dat zijn of haar gegevens binnen BPS zorgvuldig en veilig verwerkt worden. Daartoe zijn in onderhavig beleid kaders en maatregelen beschreven die de privacy binnen het verwerkingsproces waarborgen en beschermen. Dataminimalisatie en transparantie richting betrokkene zijn daarbij sleutelbegrippen. Met onderhavig beleid geeft BPS invulling aan de eisen die de Algemene Verordening Gegevensbescherming (AVG) stelt ten aanzien van de bescherming van de privacy van alle bij BPS betrokken natuurlijke personen.

1. Definities

Alle begrippen in dit beleid hebben de betekenis die daar in de AVG aan wordt gegeven.
De belangrijkste of meest voorkomende begrippen worden hieronder toegelicht:

1) persoonsgegevens:
   alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene);

2) verwerking:
   een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

3) pseudonimisering:
   het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

4) verwerkingsverantwoordelijke:
   een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;

5) verwerker:
   een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;

6) toestemming van de betrokkene:
   elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;

7) inbreuk in verband met persoonsgegevens:
   een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;

2. Verantwoordelijkheden en organisatiestructuur

BPS bepaalt het doel en de middelen van de persoonsgegevens die door of namens BPS verwerkt worden. Dit betekent dat BPS geldt als verwerkingsverantwoordelijke.

BPS heeft voor een deel van de verwerkingen de expertise van externe partijen ingeschakeld. Deze partijen verwerken de persoonsgegevens *in opdracht van BPS*. Daarmee gelden zij als verwerker in de zin van de AVG. Indien en voor zover deze verwerkers gebruik maken van andere organisaties voor de verwerking van de persoonsgegevens is sprake van subverwerkers. Deze informatie is opgenomen in het verwerkingsregister.

Onderstaande organisatieschets geeft aan hoe de verantwoordelijkheden op het gebied van privacy intern zijn verdeeld.

Het bestuur is eindverantwoordelijk. Zij stelt het privacybeleid vast, zorgt ervoor dat privacy-management onderdeel uitmaakt van de strategie, visie en bedrijfsvoering. Ze stuurt de organisatie aan en verhoogt door een actieve houding de bewustwording binnen de organisatie ten aanzien van privacy. Ook heeft zij aantoonbaar aandacht voor de wijze waarop privacymanagement wordt toegepast bij de verwerker(s) van persoonsgegevens van BPS.

BPS heeft een functionaris voor gegevensbescherming (hierna FG) aangewezen. De FG is belast met de primaire beantwoording van operationele vraagstukken op het gebied van de bescherming van persoonsgegevens. Daarnaast heeft zij een voorbereidende rol waar het de ontwikkeling van beleid, procedures of instructies op het gebied van privacy betreft. Naast deze adviserende en informerende rol, die de FG overigens ook richting de verwerker heeft, ziet de FG ook toe op de naleving van de AVG en dit privacybeleid en onderhoudt zij de contacten met de toezichthouder.

De FG rapporteert jaarlijks aan het bestuur over zijn bevindingen met betrekking tot het privacymanagement binnen BPS en bij de verwerkers. Hij heeft een directe lijn naar het bestuur en de raad van toezicht.

Daarnaast is hij op geen enkele wijze betrokken bij de operationele gang van zaken binnen BPS. BPS waarborgt zodoende de onafhankelijke positie van de FG en neemt de bepalingen uit artikel 38 AVG inzake de positie van de FG als uitgangspunt voor de samenwerking. Voor zover noodzakelijk zullen de afspraken tussen de FG en het fonds over de te verrichten werkzaamheden in een afzonderlijk document worden vastgelegd. In **Bijlage 1** is een overzicht opgenomen van de taken van de FG.

De FG onderhoudt nauw contact met de voorzitters van het bestuur (hierna dagelijks bestuur) en de risicocommissie waar het respectievelijk privacyvraagstukken of activiteiten met betrekking tot het fonds of de uitvoeringsorganisatie (PUO) betreft, danwel waar het om monitoringsactiviteiten zoals risicoanalyses of privacy gerelateerde rapportages gaat. Op deze wijze is geborgd dat binnen de aandachtgebieden van de overlegstructuren ook de (implementatie van) de privacywet- en regelgeving wordt behandeld.

Het bestuursbureau heeft een praktische ondersteunende taak bij de uitvoering van het privacybeleid. Dit betekent dat zij bijvoorbeeld op het gebied van communicatie of juridische dienstverlening het bestuur of de FG kan bijstaan maar ook dat zij assisteert bij de coördinatie van binnengekomen verzoeken van betrokkenen en eventuele klachten.

3. Verwerkingsdoeleinden en grondslagen

De informatie over natuurlijke personen die verzameld wordt door BPS, wordt gebruikt voor de volgende doeleinden:

1. Uitvoering van pensioen- en uitkeringswet- en regelgeving;
2. Vaststellen van de hoogte van en uitbetaling van pensioenaanspraken en -uitkeringen;
3. Berekenen, vastleggen en innen van premies bij werkgevers;
4. Behandelen van geschillen;
5. Voorkomen van fraude;
6. Statistische analyses;
7. Adequate communicatie met de deelnemer/betrokkene;
8. Relatiebeheer;
9. Efficiënt personeelsbeheer;
10. Websitebeheer;

Bovenstaande doeleinden moeten gezien worden in relatie tot de kerntaak van het pensioenfonds:

- Het administreren en uitvoeren van een pensioenregeling;
- Het beheren van vermogen;
- Het communiceren over bovengenoemde werkzaamheden met belanghebbenden.

De basis, of grondslag, om persoonsgegevens te verwerken voor bovengenoemde doeleinden bepaalt of de verwerking rechtmatig is. In de wet is een limitatief aantal grondslagen opgenomen. De volgende grondslagen zijn van toepassing op de verwerkingsdoeleinden van BPS:

- contractuele verplichting;
- wettelijke verplichting;
- toestemming betrokkene.

In onderstaand overzicht zijn de grondslagen gekoppeld aan de eerder genoemde verwerkingsdoeleinden.

	Contract	Wet	Toestemming
1. uitvoering van pensioen- en uitkeringswet- en regelgeving		X	
2. pensioenaanspraken en uitkeringen	X		
3. premies bij werkgevers	X		
4. geschillen	X	X	
5. voorkomen van fraude		X	
6. statistische analyses	X		
7. communicatie met de deelnemer	X	X	
8. relatiebeheer			X
9. efficiënt personeelsbeheer	X		

Gebruik van persoonsgegevens buiten het oorspronkelijke doel waarvoor ze verkregen zijn is alleen mogelijk wanneer deze verdere verwerking verenigbaar is met de doeleinden waarvoor ze oorspronkelijk verkregen zijn. Zie ook Hoofdstuk 7, Procedure nieuwe verwerkingen.

4. Dataminimalisatie

BPS beperkt de verwerking van persoonsgegevens tot wat noodzakelijk is om de doeleinden te bereiken. Daartoe vinden er periodiek analyses plaats van de (categorieën van) verwerkingen. Binnen de dataset van een verwerking wordt onderzocht of alle informatie relevant en nodig is en bekeken wordt of het doel ook met minder persoonsgegevens bereikt kan worden.
Dataminimalisatie betekent niet alleen het beperken van het verzamelen van de gegevens tot het hoogst nodige, maar ook dat de gegevens niet langer bewaard worden dan noodzakelijk voor het gestelde doel. Dit is het beginsel van opslagbeperking. BPS geeft invulling aan dit beginsel door bewaartermijnen vast te stellen voor de verwerkingen onder de verschillende doelen. De bewaartermijnen worden besproken in hoofdstuk 8.

5. Juistheid

BPS draagt er zorg voor dat de persoonsgegevens die zij verwerkt juist en actueel zijn. De volgende maatregelen worden uitgevoerd om de juistheid van de gegevens te borgen:

- Waar mogelijk verkrijgen van de benodigde gegevens direct van betrokkene;
- Periodieke navraag/verificatie ten aanzien van de juistheid van de gegevens bij betrokkene;
- Heldere instructies bij het opvolgen van signalen van onjuiste gegevensverwerking;

De FG ziet toe op de uitwerking en naleving van bovengenoemde maatregelen.

6. Transparantie

De persoonsgegevens worden te allen tijde verwerkt op een voor betrokkenen transparante wijze. Dit betekent dat de betrokkene duidelijk geïnformeerd wordt over de reden van de verwerking van de persoonsgegevens en de manier waarop. Deze gegevens, en andere relevante informatie over de verwerking van de persoonsgegevens, zijn opgenomen in de privacyverklaring van BPS. BPS draagt er zorg voor dat de privacyverklaring beschikbaar is voor de betrokkenen en op de website wordt geplaatst. De privacyverklaring is opgenomen in **Bijlage 2**.

7. Procedure nieuwe verwerkingen

Indien er ontwikkelingen plaatsvinden binnen de bedrijfsvoering van BPS die leiden tot nieuwe/andere vormen van verwerkingen dan vindt er te allen tijde voordat aanvang wordt genomen met deze verwerkingen, een onderzoek plaats naar de privacy-risico's. Het gaat daarbij bijvoorbeeld om:

- Gebruik voor een ander/nieuw doel;
- Nieuwe technologie bij het verwerken;
- Wijziging van de organisatie;
- Andere wijzigingen binnen het verwerkingsproces (bijv. uitbesteding)

Het onderzoek wordt uitgevoerd door de FG. Indien sprake is van een hoog privacy-risico wordt een Privacy Impact Assessment (PIA) uitgevoerd. De bevindingen van het onderzoek worden schriftelijk vastgelegd en gerapporteerd aan het bestuur. Het rapport bevat in ieder geval een overzicht van alle organisatorische en technische maatregelen die noodzakelijk zijn om de bescherming van de privacy binnen de organisatie op gewenst niveau te houden.

Alle verwerkingsactiviteiten worden vastgelegd in het register van verwerkingsactiviteiten. Dit register wordt schriftelijk en elektronisch opgesteld. De FG draagt er zorg voor dat het register te allen tijde actueel en volledig is. In het register zijn de volgende gegevens opgenomen:

- De naam en contactgegevens van BPS en van de FG;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en persoonsgegevens;
- De categorieën van ontvangers van de persoonsgegevens;
- De termijnen waarbinnen de verschillende categorieën gegevens worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

8. Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor het doel waarvoor zij worden verwerkt. Dit betekent dat alle persoonsgegevens die betrekking hebben op het uitvoeren van de pensioen- en uitkeringswet, inclusief de premie-inning, geschillenbehandeling en communicatie bewaard blijven voor zolang de betrokkene gebruik maakt van, aanspraak heeft op, dan wel enig ander recht heeft ten aanzien van pensioenregeling, plus een periode van 7 jaar[1] na afloop van dit gebruik of aanspraak of enig ander recht (in verband met bewijslast/administratieplicht/rechten van betrokkenen e.d.).

Ook voor de overige doeleinden is de bewaartermijn vastgesteld op 7 jaar nadat het doel van de verwerking is bereikt. Dit om aan overige wettelijke verplichtingen te kunnen voldoen zoals de belastingwetgeving, toezichtwetgeving en wetgeving inzake personeels- en arbogegevens.

BPS draagt er zorg voor dat de bewaartermijnen gehandhaafd worden. Daartoe zal een nader protocol worden opgesteld. Geautomatiseerde vernietiging waar mogelijk is daarbij het uitgangspunt. Ook de fysieke opslag van persoonsgegevens wordt in het protocol uitgewerkt. Daar geldt het principe van beperkte, geautoriseerde toegang.

Benadrukt zij dat in het geval van geschillen een vernietigingsverbod geldt ten aanzien van de betrokken relevante persoonsgegevens.

9. Rechten betrokkenen

BPS heeft de nodige maatregelen getroffen zodat de rechten van betrokkenen binnen de privacywetgeving effectief tot uitvoering kunnen worden gebracht. Het betreft de volgende rechten:

- Het recht op inzage: iedere betrokkene kan BPS vragen om inzage in de verwerking van zijn persoonsgegevens.
- Het recht op rectificatie, verwijdering, beperking of afscherming: iedere betrokkene heeft het recht om rectificatie van onjuiste persoonsgegevens of aanvulling van onvolledige persoonsgegevens te verkrijgen. Ook het verzoek van betrokkene om gegevens (deels) te wissen of af te schermen zal door BPS worden ingewilligd mits er geen wettelijke bepaling met beperkende werking op de uitoefening van dit recht van toepassing is.
- Het recht op overdraagbaarheid: iedere betrokkene heeft het recht zijn persoonsgegevens die door BPS worden verwerkt te ontvangen en over te dragen aan een andere verwerkingsverantwoordelijke;
- Het recht op bezwaar: iedere betrokkene heeft het recht om bezwaar te maken tegen de gegevensverwerking. BPS staakt de gegevensverwerking tenzij er sprake is van een dwingende, gerechtvaardigde grond die gelet op de omstandigheden zwaarder dient te wegen dan het belang van betrokkene.
- Het recht om niet aan geautomatiseerde besluitvorming te worden onderworpen.

[1] De 7 jaar gaan tellen op het moment dat de allerlaatste rechthebbenden zijn overleden.

Betrokkenen kunnen op de website en in de privacyverklaring lezen hoe zij gebruik kunnen maken van bovenstaande rechten. Daarnaast geldt dat voor ieder recht een procedure /nadere instructie wordt opgesteld waaruit duidelijk blijkt wie binnen de organisatie verantwoordelijk is voor een effectieve uitvoering van het bedoelde recht, welke termijnen hierbij in acht dienen te worden genomen, hoe de opvolging gemonitord wordt en op welke manier (het verzoek om) de uitoefening van het recht wordt vastgelegd. Hierbij wordt nauw samengewerkt met de uitvoeringsorganisatie.

BPS draagt er zorg voor dat zij is voorbereid op specifieke verzoeken die verband houden met de uitoefening van bovengenoemde rechten.

10. Beveiligingsbeleid

Beveiliging is een cruciaal vereiste binnen het privacybeleid. Uitgangspunt is dat passende technische en organisatorische maatregelen moeten zijn getroffen om persoonsgegevens te beschermen tegen verlies en onrechtmatige verwerking. Daarom is het van belang dat een beveiligingsbeleid is vastgesteld waarin de beheersmaatregelen ten aanzien van informatiebeveiliging uiteen zijn gezet.

BPS past privacy by design toe. Dit betekent dat bij ieder verwerkingsdoel is gekeken naar dataminimalisatie en de toegepaste beveiligingsmethodieken en dat waar nodig aanpassingen of verbeteringen zijn doorgevoerd (design).

De feitelijke verwerking van de persoonsgegevens is vrijwel geheel uitbesteed aan externe deskundigen, verwerkers. BPS heeft in de verwerkersovereenkomsten met deze partijen afspraken gemaakt over het niveau van beveiliging. Deze dient doorlopend te voldoen aan de voor BPS geldende verplichtingen met betrekking tot beveiliging. BPS heeft het recht periodiek na te gaan of de maatregelen ter beveiliging van de verwerkingen nog steeds een passend beveiligingsniveau bieden.

De beveiligingsmaatregelen die zijn genomen, al dan niet binnen BPS of de verwerker, in ieder geval daar waar het verwerkingsproces van de persoonsgegevens plaatsvindt, zijn gebaseerd op de Code voor informatiebeveiliging NEN (ISO 27002).

Er zijn maatregelen getroffen ter beveiliging van de gebruikte systemen en technische infrastructuur zoals apparatuur, besturingssystemen en netwerken. Het gaat hierbij om autorisaties, encryptie, actuele beveiligingssoftware en onderhoud, logging en controle van toegang tot systemen. Ook ten aanzien van medewerkers zijn er beveiligingsmaatregelen getroffen zoals een gedragscode en screening. Zowel intern als extern zijn er geheimhoudingsafspraken gemaakt.

Incident- en continuïteitsmanagement is aanwezig binnen het verwerkingsproces van de diverse verwerkingsdoeleinden (procedure datalekken, back-up en restore plan e.d.)

BPS draagt er zorg voor dat de continuïteit van de verwerking en de kwaliteit van de beveiliging op orde is en blijft. Daartoe neemt zij aantoonbaar toereikende maatregelen, die kunnen bestaan uit certificering, een beveiligingsassessment, onderzoek door een externe deskundige of een maatregel van soortgelijke strekking.

11. Uitbesteding

Uitbesteding van verwerkingen van persoonsgegevens is uitsluitend mogelijk aan een partij die ten aanzien van de bescherming van persoonsgegevens op gelijk niveau opereert. In de verwerkersovereenkomst zijn hier afspraken over gemaakt en er zijn tevens waarborgen ingebouwd die het mogelijk maken om het privacymanagement van de uitbestedingsrelatie te monitoren, zoals de mogelijkheid tot het doen van een audit.

Zonder toestemming van BPS is het niet toegestaan gegevensverwerking door een subverwerker uit te laten voeren. BPS draagt er zorg voor dat de uitbestedingsrelatie hiervan op de hoogte is.

12. Procedure datalekken

Deze procedure beschrijft hoe te handelen binnen BPS, indien er sprake is van een datalek of wanneer een datalek vermoed wordt. De meldplicht is eveneens van toepassing op BPS, als het datalek bij een derde is ontstaan, bijvoorbeeld een uitbestedingsrelatie. Deze procedure is mede gebaseerd op de beleidsregels van de AP inzake de meldplicht datalekken.

Onder een datalek wordt verstaan:
Een inbreuk op de beveiliging van persoonsgegevens die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

Het melden van een datalek intern:
De binnen BPS werkzame persoon die een (mogelijk) datalek constateert, meldt dit datalek per omgaande bij de FG en zijn leidinggevende. Degene die melding maakt van het datalek zorgt er voor dat hij alle informatie en aanwezige stukken aan de FG beschikbaar stelt. De melder is open, eerlijk en volledig over het incident.

Ook een verwerker of subverwerker kan een datalek constateren. Het is van belang dat ook in deze situatie de FG zo snel mogelijk van het datalek in kennis wordt gesteld, om die reden worden er in de desbetreffende verwerkersovereenkomsten afspraken gemaakt over de werkwijze in het geval van een datalek.

Het onderzoek:
Op basis van de verkregen informatie wordt door de FG, eventueel in overleg met het dagelijks bestuur, zo spoedig mogelijk de beoordeling gemaakt of er daadwerkelijk sprake is van een datalek.

De FG treedt in overleg met het dagelijks bestuur over het vervolgonderzoek en gezamenlijk wordt beoordeeld of er per direct maatregelen genomen moeten worden om de schade te beperken. In dit overleg wordt tevens bepaald of er gemeld moet worden aan de AP. Een dergelijke melding dient uiterlijk 72 uur nadat kennis is genomen van het datalek plaats te vinden.

Het onderzoek van de FG heeft tot doel waarheidsvinding, beperken van (mogelijke) schade en eventueel herstel in de beheersing van de bedrijfsvoering. Van het onderzoek wordt een schriftelijk verslag gemaakt. Dit rapport bevat een kort relaas van feiten en omstandigheden, bewijsvoering en advies met betrekking tot de te nemen maatregelen. In het belang van het onderzoek kunnen eventueel externe deskundigen worden ingeschakeld.

De afhandeling:
Uitgangspunt is dat de FG het onderzoek binnen een week nadat de melding van het datalek is ontvangen het onderzoek heeft afgerond en een advies heeft opgesteld. Dit eindrapport wordt besproken met het dagelijks bestuur waarna de verbetermaatregelen definitief worden vastgesteld. Tijdens deze eindbespreking wordt tevens besloten of betrokkenen geïnformeerd worden over het datalek.

Indien van toepassing verzorgt de FG de melding aan de AP en de betrokkenen. De FG houdt een registratie bij van de behandelde datalekken. Het bewijs van melding aan de AP maakt onderdeel uit van deze registratie.

Slotbepaling:
Deze regeling is beschikbaar voor alle binnen BPS werkzame personen. Zij zijn bekend met de inhoud van deze regeling en op de naleving van de procedure wordt toegezien door de FG. Deze regeling zal door de FG periodiek worden beoordeeld op actualiteit en zo nodig worden aangepast.

13. Geschillen

Wanneer een betrokkene het niet eens is met de manier waarop BPS zijn persoonsgegevens verwerkt worden of de manier waarop wordt omgegaan met de uitoefening van de rechten die betrokkene heeft op grond van de privacywetgeving, dan kan betrokkene zijn klacht hierover indienen bij de FG. BPS draagt er zorg voor dat de contactgegevens van de FG beschikbaar zijn op de website.

De FG informeert de betrokkene over de ontvangst van de klacht. Een inhoudelijke reactie dient in beginsel binnen een maand, schriftelijk, aan betrokkene te worden toegezonden. Indien nader onderzoek of informatie noodzakelijk is, kan de termijn voor afhandeling van de klacht met maximaal een maand worden verlengd. In de reactie aan betrokkene wordt betrokkene gewezen op de mogelijkheid om de klacht voor te leggen aan de AP of de rechter. De hier genoemde werkwijze wordt geïntegreerd in de klachten- en geschillenregeling van BPS.

De FG houdt een overzicht bij van de ontvangen klachten. In de jaarlijkse rapportage aan het bestuur brengt de FG verslag uit over de in het betreffende kalenderjaar ontvangen klachten.

14. Bewustwordingsprogramma

BPS draagt er zorg voor dat er periodiek binnen de organisatie trainingen en kennissessies worden georganiseerd over de privacybescherming van persoonsgegevens. De geldende interne richtlijnen, procedures en instructies worden jaarlijks besproken en zijn permanent beschikbaar. De FG formuleert eventuele andere, passende maatregelen om de privacy-awareness binnen de organisatie op gewenst niveau te houden. Voor vragen over het privacymanagement van BPS kan men terecht bij de FG.

15. Auditplan

BPS stelt ieder jaar een auditplan op. Ook privacymanagement maakt onderdeel uit van dit auditplan. Het auditplan is risico-georiënteerd en de belangrijkste controlepunten met betrekking tot het verwerkingsproces maken er in ieder geval deel van uit. De beveiliging van de systemen en data maakt in ieder geval onderdeel uit van het jaarlijks auditplan. Daarnaast zal binnen het auditplan ook aandacht moeten zijn voor de mate waarin dataminimalisatie verwezenlijkt wordt en er sprake is van doelconforme gegevensverwerking. Het auditplan kan door een interne of externe deskundige worden opgesteld en uitgevoerd. Over de bevindingen in het kader van de uitgevoerde audits wordt schriftelijk gerapporteerd aan het bestuur.

16. Evaluatie

Het privacybeleid wordt door de FG periodiek geëvalueerd en beoordeeld op effectiviteit. Waar nodig zal het beleid worden aangepast en geactualiseerd.

Bijlage 1: de taken van de functionaris gegevensbescherming

Taak
Het bestuur informeren over (wijzigingen in) privacywet- en regelgeving.
Het bestuur adviseren over (wijzigingen in) privacywet- en regelgeving.
Het informeren en adviseren van binnen het verwerkingsproces betrokken organisaties (verwerker) over (wijzigingen in) privacywet- en regelgeving.
Toezien op de naleving van de privacywet- en regelgeving binnen het fonds: – Toewijzing van verantwoordelijkheden – Bewustmaking en opleiding – Audits
Toezien op naleving van de privacywet- en regelgeving bij uitbestedingspartijen (verwerkers) – Toewijzing van verantwoordelijkheden (contract) – Bewustmaking en opleiding – Audits
Toezien op naleving van het interne privacybeleid: (inclusief het monitoren van de onderdelen die externe werking hebben) - dataminimalisatie - juiste en actuele gegevens - transparante werkwijze verwerking - onderzoek privacy risico's bij nieuwe verwerking - bijhouden verwerkersregister - juiste bewaartermijn - effectieve uitvoering van rechten betrokkenen - technische en organisatorische beveiligingsmaatregelen - toestemming uitvoering door subvewerkers - procedure datalekken - klachten verwerking persoonsgegevens - periodieke bewustwording - leveren input auditplan - periodieke evaluatie privacybeleid
Het adviseren met betrekking tot de gegevensbeschermingseffect-beoordeling (PIA) en het toezien op de uitvoering van deze beoordeling.
Eerste aanspreekpunt voor betrokkenen m.b.t. de privacywet- en regelgeving.
Contactpersoon van de Autoriteit Persoonsgegevens (AP).

Bijlage 2: privacyverklaring