Introductie

Deze vragenlijst bevat alle vragen die ingevuld kunnen worden bij het PIA-AVG zelf assessment. Afhankelijk van uw antwoorden zullen sommige vragen in de online PIA (Privacy Impact Assessment) niet aangeboden worden. Aan het eind van elk hoofdstuk is ruimte geboden om eventueel commentaar en toelichtingen te geven. Deze ruimte zal ook in de online PIA geboden worden, en meegenomen worden in de rapportage.
U kunt deze vragenlijst het best samen of in overleg met uw collega's invullen. Hierna kunt u de door u gegeven antwoorden overnemen in onze online module, opdat u een rapport van ons ontvangt. Wij verwerken ingevulde vragenlijsten volledig automatisch, het is derhalve ook niet mogelijk deze geprinte vragenlijst per post toe te zenden.

Uw gegevens

Uw Naam:
Uw Bedrijfsnaam:
Project / Systeem:
Invul datum:

Hoofdstuk Het type project

Vraag	Notitie	ja	nee	nvt
Is er sprake van het verweken van persoonsgegevens?				
Is het duidelijk wie verantwoordelijk is voor de verwerking van de gegevens?	Houd bij de beantwoording rekening met: 1) Voor en door wie het project wordt uitgevoerd. 2) Of er iemand formeel verantwoordelijk is voor de verwerking van de gegevens. 3) Of er een intern contactpersoon is.			
Verwerkt uw organisatie de persoonsgegevens in opdracht en onder verantwoordelijkheid van een andere organisatie? Ofwel: Treedt uw organisatie op als bewerker?	Deze vragenlijst is bedoeld voor organisaties die persoonsgegevens verwerken in de rol van verantwoordelijke. Deze vragenlijst is niet bedoeld voor organisaties die persoonsgegevens verwerken in de rol van bewerker			
Is het duidelijk wie na afloop van het project verantwoordelijk is voor het in stand houden en evalueren van de getroffen maatregelen?	Uiteraard moeten ook in de toekomst getroffen maatregelen in stand gehouden worden en moet worden gezorgd dat de risico's worden beheerst (bijvoorbeeld door deze PIA periodiek uit te voeren)			
Is het doel van de verwerking van persoonsgegevens binnen het project voldoende SMART omschreven?	SMART staat voor: Specifiek; de doelstelling moet eenduidig zijn Meetbaar; onder welke (meetbare/observeerbare) voorwaarden of vorm is het doel bereikt. Acceptabel; of deze acceptabel genoeg is voor de doelgroep en/of management; Is er iemand verantwoordelijk voor het realiseren van het doel? Realistisch; of de doelstelling haalbaar is. Tijdgebonden; wanneer (in de tijd) het doel bereikt moet zijn.			
Is er sprake van:				
Gebruik van nieuwe technologie?	Bijvoorbeeld intelligente transportsystemen, locatie of volgsystemen op basis van GPS, mobiele technologie, gezichtsherkenning in samenhang met cameratoezicht.			
Gebruik van technologie die bij het publiek vragen of weerstand op kan roepen?	Bijvoorbeeld biometrie, RFID, behavioural targeting (profilering).			
De invoering van bestaande technologie in een nieuwe context?	Zoals cameratoezicht of drugscontrole op de werkvloer.			
(Andere) grote verschuivingen in de werkwijze van de organisatie, de manier waarop persoonsgegevens worden verwerkt en/of de technologie die daarbij gebruikt wordt?	Bijvoorbeeld het samenvoegen of koppelen van verschillende overheidsregistraties, invoering van nieuwe vormen van identificatie of vervanging van een systeem waarin persoonsgegevens worden opgeslagen.			

Een nieuwe verwerking van persoonsgegevens	Het gebruik van gegevens voor andere bedrijfsprocessen dan waarvoor ze zijn verzameld, of bredere verspreiding van de gegevens binnen of buiten de organisatie.			
Het verzamelen van meer of andere persoonsgegevens dan voorheen of een nieuwe manier van verzamelen.	Bijvoorbeeld gegevensverrijking door enquêtes en klantonderzoeken of benadering van klanten of burgers op basis van beschikbare gegevens voor nieuwe producten of diensten.			
Gebruik van al verzamelde gegevens voor een nieuw doel of een nieuwe manier van gebruiken.	Bijvoorbeeld het samenvoegen van interne databases om klantprofielen op te stellen.			
Heeft u op alle bovenstaande (a t/m g) nee geantwoord?				
Is er (naast de Wbp) veel wet- en regelgeving ten aanzien van persoonsgegevens waar het project mee te maken heeft?	Houd bij de beantwoording rekening met: 1) Sectorale wetgeving. 2) Gedragscodes. 3) Algemene maatregelen van bestuur. 4) Jurisprudentie. 5) Internationale aspecten			
Zijn er veel maatschappelijke belanghebbenden?	Houd bij de beantwoording rekening met: 1) Medewerkers, afnemers, leveranciers, belangengroeperingen, burgers, klanten toezichthouders. 2) Welke beroepsgroepen betrokken zijn bij de verwerking.			
Zijn er bij veel partijen betrokken de uitvoering van het project?	Houd bij de beantwoording rekening met: 1) Aannemers en dienstverleners. 2) Hardware en software leveranciers. 3) IT Service providers.			
Is er een geschillenregeling of een partij waar de betrokkene terecht kan bij vragen of klachten?				

Commentaar en Toelichting:

Hoofdstuk De gegevens

Vraag	Notitie	ja	nee	nvt
Zijn alle gegevens nodig om het doel te bereiken (worden er zo min mogelijk gegevens verzameld)?	Houd bij de beantwoording rekening met: 1. Is per data-element vastgesteld wat de toegevoegde waarde is en waarom dit noodzakelijk is? 2. Kan volstaan worden met het gebruik van alleen een ja/nee in plaats van het volledige gegeven? 3. Kan volstaan worden met het verschil tussen 2 waarden in plaats van beide waarden afzonderlijk? 4. Kan gebruikgemaakt worden van andere wiskundige methodieken (bijvoorbeeld voor het bepalen van afwijkingen)?			
Kan het doel met geanonimiseerde of gepseudonimiseerde gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)?	Door pseudonimisering, worden de direct identificerende gegevens van de betrokkene op een eenduidige wijze vervangen waardoor in de toekomst bepaalde partijen nog steeds gegevens kunnen toevoegen, maar de uniek identificerende gegevens niet meer teruggehaald kunnen worden. Door anonimisering worden alle direct en uniek identificerende gegevens verwijderd.			
Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?	Denk hierbij bijvoorbeeld ook aan geolocatie, personeelsvolgsystemen, beslisondersteuning bij het als dan niet aanbieden van producten of diensten.			
Is sprake van het verwerken van:				
Bijzondere persoonsgegevens?	De Wbp (artikel 16) noemt zogenaamde bijzondere persoonsgegevens: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.			
Uniek identificerende gegevens?	Bijvoorbeeld biometrische gegevens, vingerafdrukken, DNA-profielen.			
Wettelijk voorgeschreven persoonsnummers.	Bijvoorbeeld het burgerservicenummer (BSN).			

Andere gegevens dan hiervoor beschreven waarvoor geldt dat sprake is van een (gepercipieerde) verhoogde gevoeligheid?	Bijvoorbeeld creditcardinformatie, financiële informatie, erfrechtelijke aspecten, arbeidsprestaties of gegevens waarvoor een geheimhoudingsplicht geldt?			
Bij een van bovenstaande Ja: kan het doel met andere gegevens worden bereikt die een verminderd risico op misbruik met zich mee brengen?				
Verwerkt u gegevens over kwetsbare groepen of personen?	Bijvoorbeeld minderjarige personen, verstandelijk gehandicapten, gedetineerden, onder toezicht gestelden, mensen van wie de fysieke veiligheid in gevaar is (zie bijlage F).			
Hebben de gegevens betrekking op de gehele of grote delen van de bevolking?				

Commentaar en Toelichting:

Hoofdstuk Betrokken partijen

Vraag	Notitie	ja	nee	nvt
Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere interne partijen betrokken?	Houd bij de beantwoording rekening met: 1. Afdelingen die gebruikmaken van de gegevens. 2. Afdelingen die de gegevens verzamelen. 3. De personen die toegang hebben tot de gegevens.			
Zijn er (na afronding van het project) bij het verzamelen en verder verwerken van de gegevens meerdere externe partijen betrokken?	Houd bij de beantwoording rekening met: 1. Voor en door wie het project wordt uitgevoerd. 2. Welke partijen gebruikmaken van de gegevens. 3. Of andere partijen worden ingeschakeld voor het bereiken van het doel (wordt de verwerking van gegevens geoutsourced). 4. Of de gegevens worden verkocht. 5. Welke personen buiten de organisatie toegang hebben tot de gegevens.			
Zijn er partijen betrokken (in het project of bij de verwerking) die zich niet aan een met Nederland vergelijkbare privacywetgeving hoeven te houden?	Voor gegevens die worden verwerkt buiten de Europese Economische Ruimte (EER) moet een adequaat niveau van bescherming geboden worden. Alle landen binnen de EER dienen te voldoen aan de Europese gegevensbeschermingsrichtlijn. De Europese Commissie neemt een beslissing over het passend zijn van het geboden beschermingsniveau voor landen buiten de EER. Houd bij het beantwoorden van deze vraag rekening met: 1. Of de gegevens van het grondgebied komen waar ze worden opgeslagen. 2. Of de gegevens aan partijen worden verstrekt die niet op het grondgebied zijn gevestigd waar de gegevens worden verzameld.			

Is de verstrekking van de gegevens aan derde partijen in lijn met het doel waarvoor de gegevens oorspronkelijk zijn verzameld?	Houd bij de beantwoording rekening met: 1. Wat het/de doel(en) is/zijn voor het gebruik van de gegevens. 2. Welke gegevens aan welke partijen worden verstrekt voor welk doel. 3. Of de verstrekking aan de andere partijen een wettelijke verplichting is. 4. Of de gegevens verkocht worden aan andere partijen. 5. Of andere partijen ingeschakeld worden voor het bereiken van het doel (outsourcing). 6. Hoe vaak (frequentie) worden de gegevens aan andere partijen verstrekt (eenmalig, periodieke update, continue). 7. Op welke wijze gegevens worden verstrekt aan andere partijen. 8. Of wordt vastgelegd aan welke partijen gegevens worden verstrekt. 9. Of de andere partij soortgelijke gegevens ontvangt op basis waarvan te herleiden valt op wie de gegevens betrekking hebben (indien deze geanonimiseerd of gepseudonimiseerd zijn)			
Worden de gegevens verkocht aan derde partijen?	De Wbp stelt voorwaarden aan het gebruik van gegevens voor commerciële of charitatieve doelen, zoals het recht van verzet.			

Commentaar en Toelichting:

Hoofdstuk Verzamelen van gegevens

Vraag	Notitie	ja	nee	nvt
Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden?	Houd bij de beantwoording rekening met of de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens.			
Verzamelt u de gegevens op basis van een van de wettelijke grondslagen?	De Wbp kent een beperkt aantal grondslagen op basis waarvan gegevens mogen worden verwerkt: 1. U vraagt toestemming. 2. De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is. 3. De gegevens zijn nodig voor het volgen van een wettelijke verplichting. 4. De betrokkene heeft er een vitaal belang bij dat u de gegevens verzamelt. 5. De gegevens zijn nodig voor de goede vervulling van een publiekrechtelijke taak. 6. U heeft een gerechtvaardigd belang bij de verwerking.			
Is duidelijk of u de gegevens verzamelt op basis van opt-in (verzameling uitsluitend als de betrokkene daarvoor toestemming heeft gegeven) of op basis van opt-out (verzameling tenzij de betrokkene daartegen bezwaar heeft gemaakt)?	Bij het verwerken van de gegevens moet duidelijk zijn of de betrokkene toestemming moet geven (opt-in) of dat niet hoeft, maar later bezwaar kan maken (opt-out)			
Indien u toestemming aan de betrokkene vraagt (opt-in), kunnen de betrokkenen de toestemming op een later tijdstip intrekken (opt-out)?	Deze toestemming moet een vrije, specifieke en op informatie berustende wilsuiting zijn.			
Is de impact van het intrekken van de toestemming groot voor de betrokkene?	Bijvoorbeeld omdat de dienstverlening aan de betrokkene stopgezet wordt terwijl deze daarvan afhankelijk is.			

Meldt u de betrokkene dat de gegevens worden verzameld?	Houd bij de beantwoording rekening met: 1. Waar de gegevens vandaan komen (van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera). 2. Op welke wijze de gegevens worden verzameld. 3. De mogelijkheid dat de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 4. De mate waarin de betrokkene wordt geïnformeerd. 5. De gebruikte technologie. 6. Wat het doel is/doelen zijn voor het gebruik. 7. Of de gegevens of uitkomsten van gegevensbewerking intern binnen het bedrijf verspreid worden. 8. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) de gegevens aan andere partijen worden verstrekt. 9. Hoe lang de gegevens worden bewaard.			
Bij Nee: kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens?				
Bij Ja (op vraag 4.5): meldt u de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)?				
Bij Ja: (op vraag 4.5): meldt u de betrokkene aan wie de gegevens worden verstrekt (daar waar dit geen wettelijke verplichting is)?				
Zou de betrokkene kunnen worden verrast door de verwerking (op het moment dat hij daarover wordt geïnformeerd)?	Houd bij de beantwoording rekening met: 1. De mate waarin de betrokkene wordt geïnformeerd. 2. Hoe de gegevens worden verzameld (langs welke weg). 3. De gebruikte technologie. 4. De mogelijkheid dat de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 5. Waar de gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Wat het doel is / de doelen zijn voor het gebruik. 7. Of de gegevens of uitkomsten van gegevensbewerking intern binnen het bedrijf verspreid worden. 8. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) de gegevens aan andere partijen worden verstrekt. 9. Hoe lang de gegevens worden bewaard.			

Commentaar en Toelichting:

Hoofdstuk Gebruik van gegevens

Vraag	Notitie	ja	nee	nvt
Is het gebruik van de gegevens verenigbaar (in lijn) met het doel van het verzamelen?	Houd bij de beantwoording rekening met: 1. Wat het verzameldoel is. 2. Waarvoor de gegevens worden gebruikt. 3. Welke gegevens worden verzameld. 4. Of deze gegevens bijzondere gegevens betreffen. 5. Waar de gegevens vandaan komen, van de betrokkene, een interne afdeling, een andere partij, uit eigen waarneming, et cetera. 6. Hoe vaak (frequentie) de gegevens worden verzameld (eenmalig, regelmatig of voortdurend). 7. Op welke wijze (mondeling, schriftelijk, automatisch, elektronisch, waarneming, papier) de gegevens worden verzameld en verspreid. 8. Welke afdelingen/personen en andere partijen toegang hebben tot de gegevens.			
Worden de gegevens gebruikt voor andere bedrijfsprocessen of doelen dan waar ze oorspronkelijk voor verzameld zijn?				
Past het doel van dit bedrijfsproces bij het oorspronkelijke doel van verzamelen?				
Is de kwaliteit van de gegevens gewaarborgd, dat wil zeggen: zijn de gegevens actueel, juist en volledig?	Houd bij de beantwoording rekening met: 1. Of de gegevens worden gecontroleerd, op welke wijze en op welke aspecten de controle plaatsvindt. 2. Of de gegevens kunnen worden gecorrigeerd. 3. Welke personen toegang hebben tot de gegevens voor correctie, verwijderen et cetera van de gegevens. 4. Welke afdelingen toegang hebben tot de gegevens. 5. Hoe vaak de gegevens worden geüpdatet. 6. Wat de gevolgen zijn van het gebruiken van onjuiste gegevens. 7. Of maatregelen getroffen worden om ander gebruik dan het beoogde te voorkomen. 8. Of kwaliteitswaarborgen worden verstrekt bij verstrekking van de gegevens. 9. Wat er gebeurt als (delen van) de gegevens niet aan de andere partijen worden verstrekt.			
Worden op basis van de gegevens beslissingen genomen over de betrokkenen?				

Bij Ja: leveren de gegevens een volledig en actueel beeld van de betrokkenen op?	Houd bij de beantwoording rekening met: 1. Wat het doel is van het verzamelen van de gegevens. 2. Welke gegevens (data elementen) worden verzameld. 3. Of de gegevens worden gecontroleerd (frequentie en aspecten). 4. Of de gegevens gecorrigeerd kunnen worden. 5. Hoe vaak de gegevens worden geüpdatet. 6. De wijze waarop de gegevens op betrouwbaarheid (actualiteit, volledigheid, juistheid) en relevantie (voor het doel) worden gecheckt. 7. Wat de gevolgen zijn van het gebruiken van onjuiste gegevens. 8. Of de gegevens gebruikt worden om profielen op te stellen. 9. Of de profielen op individueel niveau opgeslagen worden. 10. Welke profielen worden gebruikt.			
Is sprake van koppeling, verrijking of vergelijking van gegevens uit verschillende bronnen?				
Worden de gegevens breed verspreid binnen de organisatie?	Houd bij de beantwoording rekening met: 1. Welke afdelingen toegang hebben tot de gegevens. 2. Welke personen toegang hebben tot de gegevens. 3. De doelen en het gebruik van de gegevens.			
Worden de gegevens verspreid buiten de organisatie?	Houd bij de beantwoording rekening met: 1. Welke organisaties en personen toegang tot de gegevens hebben. 2. Hoe vaak (frequentie) de gegevens worden verstrekt. 3. Het medium dat gebruikt wordt voor verspreiding (bv. papier, CD-ROM, geheugenstick, email, internet). 4. De maatregelen om ander gebruik te voorkomen.			

Is het doorgeven van de gegevens aan partijen buiten de organisatie in lijn met de verwachtingen van het individu?	Houd bij de beantwoording rekening met: 1. Voor en door wie het project wordt uitgevoerd. 2. Wat voor technologie wordt gebruikt. 3. Of de betrokkene redelijkerwijs op de hoogte kan zijn van de verwerking van de gegevens. 4. Of de betrokkenen toestemming geven om de gegevens te verzamelen. 5. Wat het doel is / de doelen zijn voor het gebruik. 6. Of alle gegevens noodzakelijk zijn voor het doel. 7. Welke personen toegang hebben tot de gegevens. 8. Andere partijen die ook gebruikmaken van de gegevens. 9. Welke gegevens (data elementen) aan andere partijen worden verstrekt. 10. Hoelang de gegevens bewaard worden nadat ze voor het (primaire) doel zijn gebruikt.			
Stelt uw organisatie profielen op van de betrokkenen, al dan niet geanonimiseerd?	Denk hierbij aan profielen op basis van het gebruik van diensten, de afname van producten of bepaalde combinaties van eigenschappen.			
Indien profielen worden opgesteld, kan het profiel tot uitsluiting of stigmatisering leiden?	Houd bij de beantwoording rekening met: 1. Of de profielen op individueel niveau opgeslagen worden. 2. Op basis van welke gegevens de profielen worden opgesteld. 3. Welke profielen worden gebruikt. 4. Of een automatische beslissing gebaseerd wordt op de gegevens. 5. Wat de logica achter deze beslissing is. 6. Partijen aan wie de gegevens worden verstrekt.			
Kunnen de betrokkenen hun gegevens inzien of daarom vragen?	Hierbij kan gedacht worden aan reactie op verzoeken of het geven van inzage in de eigen gegevens door middel van een informatiesysteem (waarbij wel moet vast staan dat gegevens alleen ingezien kunnen worden door personen die dat mogen).			
Kunnen de betrokkenen hun gegevens corrigeren of daarom vragen (verbeteren, aanvullen)?	Hierbij kan gedacht worden aan het vragen van een reactie op opgestuurde overzichten of het geven van (eigen) correctiemogelijkheden in de eigen gegevens door middel van een informatiesysteem (waarbij de betrokkene wel op een toereikende wijze geïdentificeerd dient te worden).			

Kunnen de betrokkenen hun gegevens verwijderen of daarom vragen?	Hierbij kan gedacht worden aan een reactie op verzoeken of het geven van verwijderingsmogelijkheden in de eigen gegevens door middel van een informatiesysteem (waarbij wel moet vast staan dat gegevens alleen verwijderd kunnen worden door personen die dat mogen).			

Commentaar en Toelichting:

Hoofdstuk Bewaren en vernietigen

Vraag	Notitie	ja	nee	nvt
Is een bewaartermijn voor de gegevens vastgesteld?	Houdt hierbij rekening met het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt en bedrijfsrichtlijnen en wettelijk vastgestelde bewaartermijnen zoals bijvoorbeeld in de Archiefwet en belastingwetgeving.			
Kunnen de gegevens na afloop van de bewaartermijn fysiek worden verwijderd (uit een bestand) of vernietigd (papier)?	Het is niet voldoende om gegevens aan te merken als 'verlopen'; na het aflopen van de bewaartermijn dienen deze daadwerkelijk verwijderd te worden. Houd bij de beantwoording van de vraag rekening met: 1. Of het mogelijk is (delen van) de gegevens te vernietigen of te verwijderen. 2. Indien de gegevens worden vernietigd of verwijderd, of dit ongedaan kan worden gemaakt. 3. Of de gegevens anoniem kunnen worden gemaakt om ze te bewaren.			
Zo ja (op vraag 6.2), worden de gegevens na verstrijken van de bewaartermijn op zo'n manier vernietigd of verwijderd dat ze niet meer te benaderen en te gebruiken zijn?	Houd bij de beantwoording rekening met: 1. Of regelgeving of beleid bestaat voor de vernietiging van gegevens (bijvoorbeeld de Archiefwet). 2. Waar (welke locatie) de gegevens worden bewaard. 3. Op welk medium (papier, CD, harde schijf) de gegevens worden bewaard. 4. Of deze locatie / dit medium zijn afgeschermd voor gebruik (bijvoorbeeld het archief). 5. Welke andere redenen bestaan om de gegevens te bewaren zoals bedrijfshistorische, wettelijke, juridische redenen.			

Commentaar en Toelichting:

Hoofdstuk Beveiliging

Vraag	Notitie	ja	nee	nvt
Is sprake van intern geformuleerd beleid over het beveiligen van informatie?	Houd bij de beantwoording rekening met: 1. Of iemand verantwoordelijk is voor dit beleid. 2. Of wordt aangesloten bij algemene beveiligingsstandaarden. 3. Of rekening wordt gehouden met het bijzondere of gevoelige karakter van gegevens. 4. Of het beveiligingsbeleid wordt getoetst.			
Zo ja (op vraag 7.1), is duidelijk met welke maatregelen er voor wordt gezorgd dat aan de gestelde eisen in het beveiligingsbeleid voldaan gaat worden?	Denk hierbij aan welke maatregelen getroffen worden om te voldoen aan het beschreven beleid (een informatiebeveiligingsplan).			
Zo ja, is bij het vaststellen van de maatregelen rekening gehouden met de Richtsnoeren Beveiliging van persoonsgegevens die de Autoriteit persoonsgegevens heeft gepubliceerd?	De Richtsnoeren Beveiliging van persoonsgegevens leggen uit hoe de Autoriteit persoonsgegevens bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. In de Richtsnoeren wordt verwezen naar en aangesloten bij algemeen geaccepteerde beveiligingsstandaarden, zoals bijvoorbeeld ISO/IEC 27001/27002 en NEN 7510.			

Commentaar en Toelichting:

Hoofdstuk Meldplicht datalekken

Vraag	Notitie	ja	nee	nvt
Zijn maatregelen getroffen om datalekken indien noodzakelijk te melden aan de Autoriteit persoonsgegevens en aan de getroffen personen van wie de gegevens zijn gelekt?	In de Wbp is een meldplicht opgenomen voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken onder bepaalde voorwaarden moeten melden aan de Autoriteit persoonsgegevens en in bepaalde gevallen ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt.			
Zo ja, is bij het vaststellen van de maatregelen rekening gehouden met de Richtsnoeren die de Autoriteit persoonsgegevens over de meldplicht datalekken heeft gepubliceerd?	Organisaties tot wie de meldplicht datalekken zich richt moeten zelf een beredeneerde afweging maken of een concreet datalek (inclusief datalekken bij bewerkers) dat hen ter kennis komt onder het bereik van de wettelijke meldplicht valt. Doel van de richtsnoeren is om hen daarbij te ondersteunen. Deze richtsnoeren dienen tevens als uitgangspunt voor de Autoriteit persoonsgegevens bij het toepassen van handhavende maatregelen.			

Commentaar en Toelichting: