	A	B	C	D	E	F
1	**Toetsmodel PIA Rijksdienst**			**Gegevensrelatie SVB - Budgethouder**		
2	**Onderdeel**	**#**	**Toetsvraag**	**Wetsvoorstel WLZ**	**Risico's**	**Opmerkingen bij huidige gang van zaken**
3	**I**		**Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/ gegevensminimalisering**			
4		1	Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?	De SVB (het SVB Servicecentrum PGB (SSP)) wil als verantwoordelijke de regeling voor PGB trekkingsrechten gaan uitvoeren op grond van de WLZ (artikel 3.3.3, vijfde lid) en gaat daarvoor persoonsgegevens van de budgethouder verwerken. Deze persoonsgegevens inclusief het BSN krijgt SSP van het Zorgkantoor door toezending van de toekenningsbeschikking PGB voor zover die gegevens noodzakelijk zijn voor de de betalingen ten laste van de persoonsgebonden budgetten en het daarmee verbonden budgetbeheer (art. 9.1.3., eerste lid, onderdeel c). Het gaat daarbij in beginsel alleen om financiële gegevens van het Zorgkantoor met een uitsplitsing naar zorgprofiel. Bij de taken als trekkingsrechtuitvoerder zal de SVB de gegevens krijgen die nodig zijn om de persoon te kunnen identificeren en de gegevens inzake de hoogte van het persoonsgebonden budget, de aanwendingsrichting van het budget, de partij die het budget heeft toegekend, de contracten die de budgethouder sluit met de hulpverleners en de rekeningen van de hulpverleners (mvt artikel 9.1.3).	De zorginhoudelijke gegevens die aan het PGB ten grondslag liggen behoren niet aan de SVB te worden verstrekt. De vraag is of het aan de SVB gegeven inzicht in de aanwendingsrichting van het budget niet het risico oplevert dat SVB toch bijzondere persoonsgegevens met een zorginhoudelijk karakter verwerkt. Alles wat bij de verwerking door de SVB verder gaat dan de uitvoering van het louter financiële budgetplan dat bij het pgb behoort, is bovenmatig/niet toegestaan in de zin van de Wbp gezien ook de beperking die is opgenomen in art. 9.1.3, eerste lid, onderdeel c WLZ..	De huidige gang van zaken (de pilot 2014) laat zien dat er in de praktijk nog onduidelijkheid is over de vraag waar de zorgplicht ten behoeve van de budgethouder wordt uitgevoerd. In de mvt wordt de zorgplicht en service aan verzekerden bij het zorgkantoor gelegd. Het servicecentrum PGB vervult daar in de huidige praktijk ook een belangrijke rol in. Dezelfde onduidelijkheid is er met betrekking tot de rol in de fraudebestrijding met betrekking tot de pgb. De mvt schrijft dat elk zorgcontract op voorhand door zorgkantoor (zorginhoudelijk) en SVB is gekeurd, ondermeer om te bezien of er geen sprake is van tussenkomst van malafide bemiddelingsbureaus en zorgaanbieders. Het verwerken van een zorgcontract waarin zorginhoudelijke gegevens zijn vermeld, is naar onze mening niet noodzakelijk voor de rol die de SVB bij het pgb vervult. De SVB zou zich moeten beperken tot het verwerken van de financiële gegevens en de daarbij behorende persoonsgegevens. N.B. In artikel 2.2.2 WLZ wordt de SVB niet genoemd, de SVB behoort evenmin tot de zorgketen.
5		2	**Andere specifieke persoonsgegevens?**			

	A	B	C	D	E	F
6		2a	Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?	Nee	.	
7		2b	Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?	De toelichting hier op in het PIA model Rijksdienst luidt: hieronder vallen bijvoorbeeld minderjarigen, verstandelijk gehandicapten, mensen die te maken hebben met stalking, klokkenluiders of informanten voor politie of het OM. Dit is geen limitatieve opsomming, dus gezien het feit dat het bij de pgb gaat om groepen personen, die zorg en/ of begeleiding behoeven, kan gesteld worden dat dit een kwetsbare groep personen is.	Het risico bestaat dat er gegevens worden verwerkt, waarin de kwetsbaarheid van de budgethouder ruimere bekendheid krijgt dan nodig is.	Dit aspect pleit ervoor de gegevensuitwisseling in de verhouding SVB budgethouder zo sober mogelijk te houden.
8		2c	Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?	De WLZ laat ruimte voor de SVB om de budgethouder toe te laten tot een MijnPgb.	Door onzorgvuldig beheer van gebruikersnamen, wachtwoorden en andere inloggegevens bestaat het risico dat ongeautoriseerde toegang tot persoonsgegevens wordt verkregen.	Het risico kan hier worden beperkt door de informatie over de rekening courant positie schriftelijk uit te wisselen of via de mail.
9		2d	Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?	Nee, dit is niet de bedoeling.		

	A	B	C	D	E	F
10		2e	Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?	Artikel 2.2.2 1. De verzekerde die zich ingevolge artikel 2.2.1, tweede lid, bij een Wlz-uitvoerder aanmeldt ter inschrijving, vermeldt daarbij zijn burgerservicenummer. Artikel 9.1.1. lid 3 Bij gegevensuitwisseling tussen de Wlz-uitvoerders en de in de artikelen 9.1.2 tot en met 9.1.5 genoemde personen en instanties wordt voor zover die personen en instanties tot gebruik van dat nummer bevoegd zijn, het burgerservicenummer gebruikt. De SVB behoort tot de bedoelde instanties op basis van artikel 9.1.3 , eerste lid, onder c. De SVB wordt in onderdeel c genoemd, zodat de SVB over de noodzakelijk gegevens kan beschikken voor de uitvoering van het trekkingsrecht (artikel 3.3.3, vijfde lid) en als verantwoordelijke van de verzekerdenadministratie (artikel 35 van de Wet structuur uitvoeringsorganisatie werk en inkomen). (M v T).	Het wetsvoorstel sluit niet uit (noch regelt) dat aanbieders de beschikking krijgen over het bsn van de betrokkene. De beschikbaarheid van het bsn stelt organisaties in staat betrokkenen uniek te identificeren en om gegevens uit verschillende databanken te koppelen. Het risico bestaat dat in strijd met de Wet algemene bepalingen burgerservicenummer aanbieders in staat worden gesteld ook het bsn van de betrokkene te verwerken.	Zie onder 3 en 4

	A	B	C	D	E	F
11		3	Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? (Licht per te verwerken persoonsgegeven toe.)	Bij de taken als trekkingsrechtuitvoerder zal de SVB de gegevens moeten krijgen die nodig zijn om de persoon te kunnen identificeren, de hoogte van zijn persoonsgebonden budget, de aanwendingsrichting van het budget, de partij die het budget heeft toegekend, de contracten die de budgethouder sluit met de hulpverleners en de rekeningen van de hulpverleners. (M v T artikel 9.1.3). Gegevens omtrent de persoon Gegevens omtrent het persoonsgebonden budget. Het zou wellicht minder gemakkelijk zijn de SVB te betrekken bij het op voorhand "keuren" van het zorgcontract door de SVB.	Het risico bestaat dat meer gegevens worden verwerkt dan nodig is voor het doel.	Het eerst benoemde uitgangspunt van de landelijke werkgroep trekkingsrecht bij het opstellen van "De informatievoorziening bij trekkingsrechten is : Minimale uitwisseling van gegevens. Het valt overigens op dat de SVB niet wordt genoemd in artikel 9.2.1. over beleidsinformatie terwijl de integrale benadering van het pgb juist samenkomt bij de SVB.
12		4	Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?	Ja, in de gegevensuitwisseling met de budgethouder moet worden afgezien van het uitwisselen van medische gegevens. Met het oog op de integrale benadering van het pgb dat uit verschillende componenten kan bestaan (WLZ, WMO 2015, Jeugdwet en Zorgverzekeringswet) is gebruik van het BSN aangewezen.		Voor de onderhavige gegevensuitwisseling kan een zorginhoudelijk deel worden gemist. Zie de beperking in art. 9.1.3, eerste lid, onderdeel c WLZ.

	A	B	C	D	E	F
13		5	In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?	Dit wetvoorstel strekt ertoe een nieuwe volksverzekering in het leven te roepen, die waarborgen biedt voor behoud of verbetering van kwaliteit van leven aan mensen die – ook met steun van de eigen omgeving – niet meer zelfredzaam kunnen zijn. (M v T). Aan het bestaande AWBZ-systeem zijn nieuwe vormen van verstrekking, uitwisseling, openbaarmaking en (meervoudig) gebruik van gegevens toegevoegd. (MvT, § 10.1). De SVB past hierbij beproefde state of the art technologie en informatiesystemen toe.	Het beleidsmatig kader kan te omvangrijk zijn. Drie decentralisaties, meerdere wetten, meerdere visies en zeer veel ketenpartijen maken het lastig om grip te krijgen op de informatiehuishouding.	Het begrip «zorgbreed informatiestelsel» is nieuw in de zorg. Het drukt echter precies uit waar het in de meerjarenaanpak om draait: het als een samenhangend geheel ontwikkelen, inrichten, beheren en onderhouden van kaders waaraan getoetst kan worden of afspraken, convenanten, standaarden, registers, knooppunten en gegevenswoordenboeken (nog) voldoen aan de eisen die gesteld worden om de publieke belangen rondom zorgbrede informatiestromen te borgen. (Kamerbrief 32 620 nr 93)

	A	B	C	D	E	F
14	**II**		**Doelbinding, koppeling, kwaliteit en profilering**			
15		1	Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?	Het doel van de invoering van pgb-trekkingsrechten en de bijbehorende gegevensuitwisseling is een robuste opzet van het wettelijke recht op pgb vorm te geven door 1) de samenhang in het pgb te bevorderen door uniformering, 2) de administratieve last voor de budgethouder te verminderen en 3) fouten, fraude en oneigenlijk gebruik tegen te gaan.	Als persoonsgegevens niet voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld is de verwerking onrechtmatig.	De wijze waarop fraude en oneigenlijk gebruik wordt vastgesteld, is nog niet in detail vastgesteld.
16		2	Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).	Zowel de doelen als de systemen en het kader worden uitgebreid.		

	A	B	C	D	E	F
17		3	Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?	Zie 1 hiervoor.		Bij deze verwerking is alleen de SVB betrokken.

	A	B	C	D	E	F
18		4	Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) de functionaris voor de gegevensbescherming, of (b) het CBP indien er geen FG is?	a. De SVB (en dus ook het servicecentrum voor het pgb) beschikt (nog) niet over een FG. b.bij het CBP zijn geen meldingen gedaan inzake verwerkingen van persoonsgegevens van budgethouders.	Een niet gemelde verwerking is in principe onrechtmatig.	Ons advies is om bij het CBP zo snel mogelijk melding te maken van de huidige verwerking van de pgb-gegevens en ook zo snel mogelijk te zorgen voor de aanstelling van een FG.
19		5	Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?	In het wetsvoorstel wordt toezicht door de Zorgautoritieit voorzien. Bovendien is sprake van in voorbereiding zijnde lagere regelgeving.	Het risico bestaat dat onvoldoende maatregelen worden genomen die een rechtmatige, behoorlijke en zorgvuldige verwerking van persoonsgegevens borgen en een onnodige verzameling van persoonsgegevens voorkomen.	

	A	B	C	D	E	F
20		6	Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel of overheids ICT-systeem verwerkte persoonsgegevens na te gaan?	De gegevensuitwisseling ten behoeve van de Wlz is grotendeels gebaseerd op de gegevensuitwisseling zoals deze onder de AWBZ plaatsvindt. Ook in de Wlz wordt er gebruik gemaakt van de AZR. Het Ministerie van VWS heeft het Zorginstituut de beheertaak van de AZR gegeven. De AZR is een systematiek voor het volgen van de cliënt in alle fasen van de Wlz-keten: van de indicatie via het toewijzen en leveren van zorg tot het vaststellen van de eigen bijdrage. De partijen die hierbij betrokken zijn, de zogenaamde ketenpartijen, wisselen in gestandaardiseerde vorm informatie uit. Elke ketenpartij geeft via de AZR de informatie door die belangrijk is voor de volgende partij in de keten. De informatie-uitwisseling vindt plaats via elektronisch berichtenverkeer. Ketenpartijen maken onderling afspraken over de te hanteren standaarden, het Zorginstituut coördineert dit proces. Als partijen er onderling niet uitkomen kan de Minister van VWS bij ministeriële regeling regels stellen over deze gegevensuitwisseling. (MvT).	Het risico bestaat dat onvoldoende maatregelen zijn genomen om te waarborgen dat persoonsgegevens juist, nauwkeurig en actueel zijn. Onjuiste gegevens levert het risico op van onjuiste beslissingen die diep in kunnen grijpen op de persoonlijke levenssfeer van betrokkenen.	In artikel 9.1.2. wordt de gegevensverstrekking tussen de ketenpartijen van de Wlz geregeld. In de huidige AWBZ wordt voor de gegevensuitwisselingen tussen de ketenpartijen, het CIZ, de zorgverzekeraar, de zorgaanbieder en het CAK via de AZR-systematiek vormgegeven. AZR staat voor “AWBZ-brede zorgregistratie” waarin de verzekerde wordt gevolgd in de fasen van de keten: het indiceren van de zorgbehoefte, het toewijzen en het leveren van de zorg en het opleggen van de eigen bijdrage (de primaire processen). De ketenpartijen hebben ieder taken en bevoegdheden in deze keten en behoeven daarvoor informatie van andere ketenpartijen. De SVB is echter geen WLZ-uitvoerder en wordt daarom afzonderlijk genoemd in art. 9.1.3, eerste lid, onderdeel c WLZ en krijgt alleen persoonsgegevens voor zover deze noodzakelijk zijn voor de betalingen ten late van de pgb's en het daarmee verbonden budgetbeheer. Dit vraagt dus extra aandacht voor de aansluiting bij de AZR-systematiek..

	A	B	C	D	E	F
21		7	Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?	In beginsel niet maar de aanpak van fraude en oneigenlijk gebruik moet nog nader worden uitgewerkt. Mogelijk moet de vraag dus te zijner tijd met ja worden beantwoord.	Het risico bestaat dat betrokkene onterecht in aanmerkelijke mate wordt getroffen door besluiten genomen op grond van gegevens vanuit verschillende aanbieders met ieder hun eigen context. Het risico bestaat dat meer gegevens worden verwerkt dan nodig voor het doel. Het risico bestaat dat persoonsgegevens verder worden verwerkt op een wijze die niet verenigbaar is met de doeleinden waarvoor ze zijn verkregen.	Het verdient aanbeveling de doelbinding op het punt van bestrijding van fraude en oneigenlijk gebruik nader uit te werken.
22		8	Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?	Dit kan nu nog niet worden beoordeeld. Zie 7 hiervoor.	Het risico bestaat dat betrokkene onterecht in aanmerkelijke mate wordt getroffen door besluiten die geautomatiseerd genomen worden zonder menselijke tussenkomst.	

	A	B	C	D	E	F
23	**III**		**Betrokken instanties/systemen en verantwoordelijkheid**			
24		1	Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?	De leverancier van het startbericht in de gegevensuitwisseling 'Trekkingsrechten"is het zorgkantoor dat het pgb heeft toegekend. Vervolgens worden er deelbestanden in het kader van het beheer van het pgb verwerkt.	Het risico bestaat dat beperkte transparantie over ontvangers en verstrekkers van gegevens, alsmede gebruikte infrastructuren en deelbestanden leidt tot minder zekerheid omtrent de betrouwbaarheid van gegevens. De betrokkene verliest na eenmalige verstrekking de grip op zijn persoonsgegevens, ook omdat sprake is van meerdere (voor de betrokkene niet-transparante) gegevensbronnen. Hierdoor ontstaat het risico dat de betrokkene gevolgen ondervindt van onjuist genomen beslissingen, bijvoorbeeld omdat deze zijn gebaseerd op verouderde of onjuiste gegevens.	De informatievoorziening richting budgethouder in 2015 moet nog worden uitgewerkt. Gezien de doelgroep vergt dit een inspanning om zo duidelijk mogelijk te communiceren over het trekkingsrechtensysteem en de acties die daarbij van de budgethouder worden verwacht.
25		2	Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?	Ja, de voorbereiding van de uitvoering door de SVB vindt in 2014 gefaseerd plaats via pilots cf. de aangepaste Regeling subsidies AWBZ. De fasering is erop gericht in 2015 het gehele systeem operationeel te hebben.	Het risico bestaat dat de SVB onvoldoende voorbereid en geëquipeerd is wat betreft de nodige voorzieningen en maatregelen en dat als gevolg daarvan de gegevensverwerking onrechtmatig is en/of dat betrokkenen gevolgen ondervinden van onterechte beslissingen.	De Sociale verzekeringsbank is de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens voor de verwerking van persoonsgegevens van WLZ-verzekerde budgethouders.

	A	B	C	D	E	F
26		3	Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?	Deze vraag is in het wetsvoorstel niet beantwoord.	Het niet opnemen van dit element vormt een risico voor de rechtmatigheid van de verwerking.	Het verdient aanbeveling dat een te benoemen FG in 2014 zorgdraagt voor een beschrijving van de beoogde beveiliging van het trekkingsrechtensysteem in 2015 en dat hij zich vergewist van tijdige realisatie van de beoogde beveiliging.
27		4	Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?	In de zorgsector geldt een uitgebreid web van geheimhoudingsverplichtingen. Voor de onderhavige uitwisselingsrelatie is van belang dat medische gegevens niet worden uitgewisseld (vgl. art. 9.1.3, eerste lid, onderdeel c). Voorts is in artikel 9.1.2 lid 6 van de WLZ geregeld dat: Personen werkzaam bij een Wlz-uitvoerder, voor wie niet reeds uit hoofde van ambt of beroep een geheimhoudingplicht geldt, zijn verplicht tot geheimhouding van de gegevens als bedoeld in het eerste of vierde lid, behoudens voor zover enig wettelijk voorschrift hen mededeling toestaat.	Het risico is hier dat niet volledig duidelijk is waar de grens moet worden getrokken op grond van art. 9.1.3, eerste lid, onderdeel c WLZ	Het verdient aanbeveling nauwkeurig er vast te leggen welke gegevens het zorgkantoor overdraagt aan de SVB ten behoeve van het trekkingsrechtensysteem.
28		5	Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?	Ja, in het Plan van Aanpak Invoering Trekkingsrechten systeem PGB (Voor AWBZ, Wmo en Jeugdwet) van de SVB in opdracht van het Ministerie van VWS. Dit is echter een intern document, dus voor betrokkenen is niet inzichtelijk bij wie, waarom en hoe de persoonsgegevens worden verwerkt.	Wanneer dit niet duidelijk in kaart is gebracht, wordt het voor de verantwoordelijke een lastigere opgave om in control te zijn en zal hij moeite hebben om de informatieplicht goed te vervullen.	Zie 4. hiervoor.

	A	B	C	D	E	F
29		6	Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?	Dit blijkt niet uit dit wetsvoorstel. Voor een beschrijving van de huidige situatie zie de rechterkolom.		Uitwisseling van gegevens mag alleen geschieden als dat wettelijk is geregeld, als dat noodzakelijk is voor de uitoefening van een publiekrechtelijke taak of als de betrokkene toestemming heeft gegeven. De naleving van de privacyregels is geïntegreerd in het informatiebeveiligingsbeleid van de SVB en de bijbehorende organisatie. Daarmee is ook de controle op die naleving verankerd. (SVB Jaarverslag 2012). Voor de beoogde situatie in 2015 zijn er echter nog onzekerheden. Zie 4 hiervoor.
30		7	Is er sprake van overdracht van persoonsgegevens naar een (overheids) instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?	Nee.		

	A	B	C	D	E	F
31	**IV**		**Beveiliging en bewaring/vernietiging**			
32		1	Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging ?	Dit staat niet in het wetsvoorstel, maar hier kan wat betreft de SVB wel naar de huidige situatie in de rechterkolom gekeken worden.	Het niet opnemen van dit element vormt een risico voor de rechtmatigheid van de verwerking.	De SVB ontwikkelt zich steeds verder tot een open netwerkorganisatie. De kwetsbaarheid en (keten)afhankelijkheid van de SVB neemt daardoor toe, in gelijke tred met externe dreigingen, met name op gebied van cybercrime. De impact van eventuele gevolgen zal daardoor ook groter worden. Om die reden is in de tweede helft van 2012 een herijking gestart van het informatiebeveiligingsbeleid van de SVB. (SVB jaarverslag 2012). Voor informatiebeveiling volgt de SVB de ISO 27001 norm volgens de roadmap invoering SVB Trekkingsrechtensysteem per 1-1-2014 versie 3.0. Zie echter ook III.3.
33		2	Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?	Niet van toepassing.		

	A	B	C	D	E	F
34		3	Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a) gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?	De SVB heft in beginsel een state of the art beschermingsniveau maar in het wetsvoorstel wordt aan dit onderwerp geen aandacht besteed.. Zie echter	Het niet opnemen van dit element vormt een risico voor de rechtmatigheid van de verwerking en voor de beveiliging van de gegevens. Een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen is vereist op basis van artikel 13 Wbp. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Ontbreken de maatregelen of zijn deze niet goed ingeregeld dat worden de risico's op een niet passend beveiligingsniveau groter, evenals de risico's op onnodige verzameling en verdere verwerking van persoonsgegevens.	Zie IV.1.
35		4	Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?	Dit wordt niet expliciet vermeld in het wetsvoorstel. Uiteraard zijn algemeen geldende voorschriften zoals de meldplicht datalekken van toepassing.	In het geval van een datalek of een andersoortige inbreuk op de beveiliging is op basis van de wet onvoldoende duidelijk wie waar verantwoordelijk voor is.	Zie IV.1

	A	B	C	D	E	F
36		5	Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?	In de WLZ ontbreekt een regeling voor bewaartermijnen cf. art. 4.3.4, eerste lid, en 4.3.5. WMO 2015.		Het verdient aanbeveling het wetsvoorstel WLZ op dit punt bij nvw aan te vullen
37		6	Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?	Zie IV.5		
38		7	Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?	Zie IV.5		

	A	B	C	D	E	F
39	**V**		**Transparantie en rechten van betrokkenen**			
40		1	Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?	Het doel is bekend op basis van de wet en de communicatie over de gewijzigde wetgeving door de zorgkantoren en de SVB.		
41		2	Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?	De SVB verkrijgt de persoonsgegevens niet direct van de betrokkene.	Het risico bestaat dat de betrokkene niet in staat wordt gesteld zijn rechten goed uit te kunnen oefenen.	De zorgkantoren moeten eerst nog hun administratie aanpassen voordat zij de pgb's over kunnen maken naar de SVB. Het zorgkantoor laat de budgethouder vooraf weten wanneer het pgb overgaat naar de SVB. Vanaf 1 januari 2015 worden alle pgb's overgemaakt aan de SVB.
42		3	Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?	De toekenningsbeschikking wordt tegelijk aan de budgethouder en de SVB toegestuurd.		

	A	B	C	D	E	F
43		4	Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?	In navolging van het advies van het CBP is de onherroepelijke toestemming die een verzekerde moest geven wilde hij in aanmerking kunnen komen voor een Wlz-indicatie, geschrapt. Zoals het CBP adviseert, is in plaats daarvan in de Wlz een artikel opgenomen op grond waarvan derden op verzoek van het CIZ verplicht zijn het CIZ die (gezondheids)persoonsgegevens te leveren, die voor het CIZ noodzakelijk zijn om een goed Wlz-indicatiebesluit te geven. In dat artikel is tevens geëxpliciteerd dat onder 'derden' mede worden verstaan hulpverleners met een medisch beroepsgeheim. Daarmee is dan tevens voorzien in een wettelijke verplichting tot gegevensverstrekking als bedoeld in artikel 7:457 van het Burgerlijk Wetboek (BW). Voorts is in dat artikel, zoals het CBP vraagt, bepaald dat het soort gezondheidsgegevens waar het om kan gaan, bij ministeriële regeling zal worden aangeduid.	Risico dat genomen maatregelen onvoldoende toereikend zijn. Het niet opnemen van bepalingen aangaande toestemming vormt een risico voor de rechtmatigheid van de verwerking.	Het verdient aanbeveling het wetsvoorstel WLZ aan te vullen met de bepaling in art. 4.3.5, eerste lid, WMO 2015
44		5	Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?	In de WLZ ontbreekt een regeling voor inzage bij de SVB cf. art. 4.3.2 WMO 2015.		Het verdient aanbeveling het wetsvoorstel WLZ op dit punt bij nvw aan te vullen

	A	B	C	D	E	F
45		6	Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?	In de WLZ ontbreekt een regeling voor inzage bij de SVB cf. art. 4.3.2, zesde lid WMO 2015.		Het verdient aanbeveling het wetsvoorstel WLZ op dit punt bij nvw aan te vullen