HANDREIKING PRIVACY COMPLIANCE

Aan	Klanten van PSO-Nederland en Gebruikers van de PSO
Van	PSO-Nederland en TNO
Betreft	Handreiking privacy compliance bij gebruik van de Prestatieladder Socialer Ondernemen (PSO)
Datum	13 april 2018

---

1 Achtergrond

1.1 Voor u ligt een handreiking privacy compliance die is opgesteld door PSO-Nederland B.V. (**PSO-Nederland**) en TNO, nadat hierover advies is ingewonnen bij het advocatenkantoor Van Doorne N.V. Deze handreiking wordt verstrekt aan u als klant van PSO-Nederland om nadere informatie te geven over hoe u privacy compliant gebruik kunt maken van de Prestatieladder Socialer Ondernemen (**PSO**). Wij stellen deze handreiking ter beschikking omdat PSO-Nederland vaak vragen krijgt van haar klanten over welke privacyverplichtingen voor hen gelden onder de Algemene verordening gegevensbescherming (**AVG**) in het kader van de PSO en hoe zij daaraan moeten voldoen. We raden u aan om deze handreiking goed te lezen en toe te passen.

1.2 Deze handreiking omschrijft alleen de belangrijkste privacyverplichtingen voor klanten van PSO in algemene zin. Het is daarom voor het waarborgen van de privacy compliance belangrijk dat u de privacyregels afstemt en toepast op uw specifieke situatie. Met het verspreiden van deze handleiding neemt PSO-Nederland geen verantwoordelijkheid op zich voor het waarborgen van de privacy compliance van haar klanten. Het blijft uw eigen verantwoordelijkheid om ervoor te zorgen dat u handelt in overeenstemming met de privacyregels, ook als u de PSO gebruikt.

Management Samenvatting

Bij het gebruik van de PSO verwerken uzelf en de door u gecontracteerde auditor gegevens over uw medewerkers. Omdat dit deels gevoelige gegevens kan betreffen over bijvoorbeeld de gezondheid van medewerkers, rijst de vraag hoe dit kan plaatsvinden in overeenstemming met de privacyregels en de AVG in het bijzonder.

Ter beantwoording van die vraag zijn in deze notitie eerst de belangrijkste privacytermen toegepast op de PSO, met daarna een algemeen overzicht van relevante privacyverplichtingen. Vervolgens wordt een mogelijk knelpunt voor de privacy compliance weergegeven, waarna enkele praktische voorbeelden als oplossing hiervoor worden genoemd.

1.3 Als u meer informatie zoekt over bepaalde plichten, kunt u de website van de Autoriteit Persoonsgegevens raadplegen op www.autoriteitpersoonsgegevens.nl. Hier kunt u ook de tekst van de AVG en verschillende toelichtingen daarop nalezen.

2 Verwerking van persoonsgegevens bij de PSO

2.1 De privacyregels zijn van toepassing op de verwerking van persoonsgegevens. Om te beoordelen of bij het gebruik van de PSO persoonsgegevens worden verwerkt, zijn de volgende definities relevant.

Persoonsgegevens

- Persoonsgegevens zijn alle gegevens die direct of indirect herleidbaar zijn tot een levende natuurlijke persoon, die de 'betrokkene' wordt genoemd.
- Voorbeelden zijn: NAW-gegevens, telefoonnummers, iemands foto, informatie over iemands ras of godsdienst, maar soms ook IP-adressen.
- Ook versleutelde gegevens zijn persoonsgegevens, zolang zij kunnen worden herleid tot individuen zodra zij zijn ontsleuteld.
- Als de gegevens volledig en onomkeerbaar zijn geanonimiseerd, is er geen sprake meer van persoonsgegevens. Dan is de AVG niet langer van toepassing. Wel dient ook dan nog rekening te worden gehouden met een eventueel afgeleid privacyrisico.

Verwerking

- Een verwerking van persoonsgegevens is een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés.
- Voorbeelden zijn het verzamelen, opslaan, wijzigen, raadplegen, gebruiken, verstrekken en vernietigen van persoonsgegevens.

2.2 Door voornoemde brede definities, is al snel sprake van het verwerken van persoonsgegevens. In het kader van het gebruik van de PSO, kan dit verwerken worden opgesplitst in de volgende drie fases:

2.2.1 *Verzamelen*. In deze voorfase vergaart u intern de informatie die nodig is voor het invullen van de online rekentool in de fase hierna.

➢ In deze fase verwerkt u (onder meer) gegevens over uw medewerkers.

2.2.2 *Invullen.* Deze fase betreft het invullen van de door u verzamelde gegevens in de online rekentool die PSO-Nederland aanbiedt. Met deze tool kunt u berekenen wat uw sociale bijdrage is, gebaseerd op verschillende kwantitatieve criteria (o.a. het aantal medewerkers met een kwetsbare arbeidsmarktpositie).

➢ In deze fase verwerkt u contactgegevens van PSO-Nederland en vice versa verwerkt PSO-Nederlands contactgegevens van u. Omdat in de rekentool alleen op geaggregeerd niveau gegevens worden opgevraagd, althans gegevens die doorgaans niet rechtstreeks tot individuen kunnen worden herleid doordat u bijv. geen NAW-gegevens over hen invult, verwerkt PSO-Nederland in principe geen persoonsgegevens over uw medewerkers.

2.2.3 *Certificeren.* Deze fase ziet op het aanvragen van een PSO-certificaat. Hier verstrekt u de in de rekentool ingevulde gegevens en inzage in aanvullende informatie aan een door u ingeschakelde auditor, verkozen uit onze voorselectie. De auditor controleert de in de rekentool ingevulde gegevens en beoordeelt of u in aanmerking komt voor een PSO-certificaat. Hij geeft deze beoordeling door aan PSO-Nederland, die op grond daarvan het PSO-certificaat wel of niet toekent.

- In deze fase verwerken u, PSO-Nederland en de auditor, contactgegevens van elkaar. Daarnaast verwerken u en de auditor persoonsgegevens over uw medewerkers.

2.3 Uit voorgaande volgt dat bij het gebruik van de PSO met name van de volgende categorieën betrokkenen persoonsgegevens worden verwerkt:

2.3.1 contactgegevens van u, PSO-Nederland en de auditor, en

2.3.2 gegevens over uw medewerkers, waaronder mogelijk ook meer gevoelige gegevens, zoals of iemand een uitkering krijgt op basis van de Wet werk en inkomen naar arbeidsvermogen (WIA).

Betrokkene

- Degene over wie persoonsgegevens worden verwerkt.

3 Privacyrollen van u als klant, PSO-Nederland en de auditor

3.1 Bij het gebruik van de PSO zijn hoofdzakelijk drie partijen betrokken: u, PSO-Nederland en de auditor. Deze partijen hebben elk een eigen privacyrol. De privacyrol is bepalend voor de privacyverplichtingen die op een partij rusten en wordt daarom op hoofdlijnen in kaart gebracht.

Verwerkingsverantwoordelijke (kortweg: verantwoordelijke)

- De partij die het doel en de (financiële) middelen van de gegevensverwerking vaststelt.
- Op de verantwoordelijke rusten meer verplichtingen dan op de verwerker.

Verwerker:

- De partij die ten behoeve van een verantwoordelijke persoonsgegevens verwerkt zonder direct aan diens gezag te zijn onderworpen.
- Met andere woorden: mogelijk wel opdrachtnemers zoals ICT-dienstverleners, maar geen medewerkers.
- De verwerker heeft zelf geen zeggenschap over de verwerking, maar voert de verwerkingsactiviteiten alleen uit op instructie van de verantwoordelijke. Het is de verwerker dan ook niet toegestaan om de persoonsgegevens ook voor eigen doeleinden te verwerken.

3.2 In het kader van het gebruik van de PSO, verwerken zowel u, PSO-Nederland als de auditor, bepaalde persoonsgegevens ten eigen behoeve. Aanname is dat u graag PSO certificering wenst, en daarom persoonsgegevens verwerkt in het kader van de PSO. U verzamelt hiertoe eerst diverse medewerkersgegevens, en vult deze in de PSO rekentool in. Vervolgens vraagt u certificering aan, kiest u een auditor uit de voorselectie van PSO-Nederland en schakelt deze in. Aldus verwerkt u voor eigen doeleinden de contactgegevens van PSO-Nederland en de auditor, en de medewerkersgegevens die nodig zijn voor het invullen van de rekentool en nadien aantonen aan de auditor dat deze juist zijn ingevuld. U bent hiervoor een verantwoordelijke naar privacyrecht.

3.3 PSO-Nederland wenst op haar beurt de PSO aan te bieden, en verwerkt in dat kader bepaalde persoonsgegevens. Aangezien u over uw medewerkers alleen gegevens aanbiedt op geaggregeerd niveau, althans gegevens die doorgaans niet rechtstreeks tot individuen kunnen worden herleid, kan PSO-Nederland in principe geen verantwoordelijke zijn voor verwerking van persoonsgegevens van uw medewerkers. Ook voor zover PSO-Nederland theoretisch in staat zou zijn om gegevens te herleiden tot individuele medewerkers, bijvoorbeeld omdat u ongevraagd extra informatie verschaft of indien uw organisatie dusdanig klein is dat het maar om één werknemer kan gaan, zal PSO-Nederland geen gebruik maken van deze mogelijkheid. Wel verwerkt PSO-Nederland voor het ter beschikking stellen van de PSO contactgegevens van zowel u als de auditor. Hiervoor is PSO-Nederland een verantwoordelijke naar privacyrecht.

3.4 De auditor wenst tot slot diens beroep uit te oefenen, en geniet daarbij een behoorlijke vrijheid ten aanzien van de manier waarop daaraan invulling wordt gegeven. De auditor bepaalt in belangrijke mate zelf hoe de audit plaatsvindt van de gegevens die zijn ingevuld in de PSO rekentool. Alhoewel de auditor is aangedragen door PSO-Nederland en handelt in opdracht van u, is daarom ook de auditor een zelfstandige verantwoordelijke naar privacyrecht.

3.5 Wel kan er een zekere mate van overlap tussen uw verantwoordelijkheid en die van de auditor bestaan. Dit betreft het deel van de audit dat bij u op de werkvloer wordt uitgevoerd. Dan is het wellicht niet mogelijk strikt te onderscheiden waar uw verantwoordelijkheid stopt en die van de auditor begint. Dit kan zich bijvoorbeeld voordoen wanneer u zelf de stukken selecteert voor de auditor, maar de auditor hiertoe op variërend detailniveau instructies verleent. Voor dit deel van de gegevensverwerking in het kader van de PSO kunnen u en de auditor dan gezamenlijke verantwoordelijke naar privacyrecht zijn.

3.6 Voorgaande toepassing op hoofdlijnen van de definities van de mogelijke privacyrollen op u, PSO-Nederland en de auditor, is hierna weergegeven in een overzicht.

Privacyrollen bij gebruik PSO	
Partij:	**Verantwoordelijk voor:**

U (klant PSO)	• Het verwerken van medewerkersgegevens:
	  ○ Het verzamelen/selecteren voor en invoeren in de PSO rekentool: zelfstandig verantwoordelijk.
	  ○ Het verzamelen, selecteren en verstrekken aan de auditor: deels zelfstandig en wellicht deels gezamenlijk met de auditor verantwoordelijk.
	• Het verwerken van contactgegevens:
	  ○ Contactgegevens van PSO-Nederland; en
	  ○ Contactgegevens van de auditor.

PSO-Nederland	• Het verwerken van contactgegevens:
	  ○ Contactgegevens van u als klant van PSO-Nederland; en
	  ○ Contactgegevens van de auditor.

Auditor	• Het verwerken van medewerkersgegevens:
	  ○ Het verwerken van de medewerkersgegevens van de klant van PSO-Nederland ter beoordeling van de PSO certificering: zelfstandig verantwoordelijk.
	  ○ Wellicht ook gezamenlijk met u als klant van PSO-Nederland verantwoordelijk voor een deel van de voorfase: het verzamelen en selecteren van medewerkersgegevens ten behoeve van het uitvoeren van de audit.
	• Het verwerken van contactgegevens:
	  ○ Contactgegevens van u; en
	  ○ Contactgegevens van PSO-Nederland.

3.7 Nu zowel u, PSO-Nederland als de auditor verantwoordelijken zijn in de zin van het toepasselijk privacyrecht, moeten al deze partijen voldoen aan de verplichtingen die de AVG op verantwoordelijken legt.

4 Algemene privacyverplichtingen

4.1 De belangrijkste privacyverplichtingen die onder de AVG gelden voor verantwoordelijken, staan in de onderstaande tabel vermeld. Omdat alleen ten aanzien van uw medewerkers ook meer gevoelige persoonsgegevens kunnen worden verwerkt, is deze handreiking met name op de privacy compliance ten aanzien van deze groep betrokkenen gericht.

Overzicht belangrijkste privacyverplichtingen	
1. Zorgvuldige verwerking	De persoonsgegevens mogen alleen worden verwerkt op een wijze die ten aanzien van de betrokkenen rechtmatig, behoorlijk en transparant is.
2. Data-minimalisatie	Er mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel van de verwerking te bereiken. De verwerking van persoonsgegevens moet toereikend, ter zake dienend en niet bovenmatig zijn (proportionaliteitseis). Daarnaast moet worden gekozen voor een werkwijze die privacytechnisch het minst ingrijpend is (subsidiariteitseis). ➢ In dit kader is het raadzaam alleen die medewerkersgegevens te verzamelen en verder te verwerken die noodzakelijk zijn voor de PSO. Zowel voor de rekentool als voor de audit dienen zo min mogelijk gegevens te worden verwerkt die herleidbaar zijn tot uw medewerkers.
3. Legitiem doel	Persoonsgegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De persoonsgegevens mogen vervolgens niet verder worden verwerkt op een manier die onverenigbaar is met die doeleinden. ➢ In dit kader is het raadzaam te waarborgen dat de medewerkersgegevens die worden verzameld en verwerkt voor de PSO niet ook voor andere doeleinden worden verwerkt.
4. Grondslag	Persoonsgegevens mogen alleen worden verwerkt als dit kan worden gebaseerd op één van de wettelijke grondslagen hiervoor in de AVG. In het kader van de PSO zijn de twee meest relevante grondslagen over het algemeen: • Het gerechtvaardigd belang: de verwerking is noodzakelijk voor een gerechtvaardigd belang, dat prevaleert boven het privacybelang van uw medewerkers (artikel 6, lid 1 sub f van de AVG); en • Toestemming van uw medewerkers. ➢ Op toepassing van de grondslagen wordt verder ingegaan onder nummer 6 van deze handreiking (artikel 6, lid 1 sub a van de AVG).
5. Bijzondere persoons-gegevens	Bijzondere persoonsgegevens zijn gegevens waarvan wordt aangenomen dat het verwerken hiervan verhoogde privacy-impact kan hebben. Dit geldt bijvoorbeeld voor gegevens over iemands gezondheid. Zulke persoonsgegevens mogen niet worden verwerkt, tenzij een specifieke wettelijke uitzondering op dit verwerkingsverbod van toepassing is, zoals uitdrukkelijke toestemming (artikel 9, lid 2, sub a van de AVG). ➢ Nu in het kader van de PSO gezondheidsgegevens van uw medewerkers kunnen worden verwerkt, moet hiermee rekening worden gehouden. Hierop wordt verder ingegaan onder nummer 5 van deze handreiking.
6. Documentatie-plicht	Onder de AVG moeten verschillende aspecten van de persoonsgegevens-verwerking intern worden gedocumenteerd, zoals welke persoonsgegevens u verwerkt voor welke doeleinden.

	➢ Het is raadzaam te verifiëren dat de verwerking van persoonsgegevens voor de PSO ook is opgenomen in uw verwerkingsregister om te voldoen aan uw documentatieplicht.
7. Informatieplicht	Uw medewerkers moeten op juiste en begrijpelijke wijze worden geïnformeerd over de verwerking van hun persoonsgegevens in het kader van de PSO. ➢ Het is raadzaam hiervoor een privacy statement op te stellen of dit onderdeel op te nemen in een bestaand privacy statement.
8. Rechten van betrokkenen	De betrokken medewerkers hebben o.a. een recht op inzage, rectificatie en bezwaar. Dit hebben zij ook in relatie tot de verwerking van hun persoonsgegevens voor de PSO. Zij moeten hiervan op de hoogte worden gesteld en als zij een verzoek indienen, moet u hierop adequaat reageren. ➢ Dit punt kan bijvoorbeeld worden meegenomen in een privacy statement (zie punt 7 hierboven).
9. Gegevens-verwerkings-overeenkomst	Partijen die gezamenlijk verantwoordelijk zijn voor de verwerking van persoonsgegevens zijn onder de AVG in principe verplicht om op transparante wijze hun respectieve verantwoordelijkheden in een onderlinge regeling vast te leggen, bijvoorbeeld in een gegevensverwerkingsovereenkomst. ➢ Het is raadzaam om te onderzoeken of u met de auditor een gegevensverwerkingsovereenkomst dient te sluiten.
10. Beveiligings-maatregelen	U moet passende beveiligingsmaatregelen treffen om ervoor te zorgen dat de persoonsgegevens veilig zijn en u moet passende organisatorische en technische beveiligingsmaatregelen nemen die ervoor zorgen dat persoonsgegevens niet verloren gaan of onrechtmatig worden verwerkt. Wat passend is, hangt af van de omstandigheden van het geval, zoals de gebruikte technieken en de gevoeligheid van de persoonsgegevens. ➢ U kunt deze webpagina van de Autoriteit Persoonsgegevens raadplegen voor voorbeelden van dergelijke maatregelen.
11. Meldplicht datalekken	Als er een ernstig datalek optreedt (als uw computersysteem bijv. wordt gehackt), dan moet u dit binnen 72 uur melden aan de Autoriteit Persoonsgegevens. In sommige gevallen moeten ook de betrokkenen van wie de persoonsgegevens zijn gelekt op de hoogte worden gesteld. ➢ Als u geen roadmap data breaches of vergelijkbaar document heeft, kunt u overwegen dit op te stellen. Niet zozeer in het kader van de PSO, maar in algemene zin.
12. Bewaar-termijnen	Persoonsgegevens mogen niet langer worden bewaard dan strikt noodzakelijk is voor het doeleinde waarvoor zij worden verwerkt. ➢ Als u geen bewaarbeleid heeft, kunt u overwegen dit op te stellen. Niet zozeer in het kader van de PSO, maar in algemene zin.
13. Doorgifte naar derde landen	Als u persoonsgegevens doorgeeft naar landen buiten de EER (bijv. doordat uw server daar staat en de gegevens daar worden opgeslagen), gelden aanvullende eisen.

4.2 Over alle bovengenoemde verplichtingen kunt u verder lezen op de website van de Autoriteit Persoonsgegevens: www.autoriteitpersoonsgegevens.nl. De Autoriteit Persoonsgegevens heeft bovendien een regelhulp AVG gepubliceerd; zie daarvoor deze webpagina.

4.3 Op twee van de bovenstaande verplichtingen gaan we hieronder nader in, omdat deze belangrijk zijn voor het verwerken van persoonsgegevens in het kader van de PSO. Dit zijn de grondslag voor de verwerking en het verbod om bijzondere persoonsgegevens te verwerken. Omdat de vraag of bijzondere persoonsgegevens worden verwerkt impact heeft op de toepasselijkheid van een grondslag, wordt dit eerst behandeld.

5 Bijzondere persoonsgegevens

5.1 Gezondheidsgegevens zijn een categorie van bijzondere persoonsgegevens. Dit zijn alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen. Ook het enkele gegeven dat iemand ziek is valt daaronder, ondanks dat dat gegeven op zichzelf niets zegt over de aard van de aandoening. De constatering dat een medewerker een lichamelijke beperking heeft, mag daarom in principe niet worden verwerkt, ondanks dat de handicap voor iedereen zichtbaar is.

5.2 In het kader van de PSO kunnen zowel door u als door de auditor gezondheidsgegevens van bepaalde medewerkers van u worden verwerkt. Hierna wordt toegelicht hoe dit invloed heeft op de keuze van de toepasselijke grondslag.

6 Grondslag van de verwerking

6.1 De AVG regelt op welke gronden persoonsgegevens mogen worden verwerkt. Dit is een strikt systeem: als er géén wettelijke grondslag zoals genoemd in artikel 6, lid 1 AVG voor verwerking van toepassing is, dan mogen de persoonsgegevens niet worden verwerkt. Voor verwerking van persoonsgegevens in het kader van de PSO zijn met name het gerechtvaardigd belang en de uitdrukkelijke toestemming van de betrokken medewerker van belang.

Gerechtvaardigd belang

6.2 Het gerechtvaardigd belang houdt in dat u een belangenafweging maakt tussen de belangen die zijn gediend met het verwerken van de medewerkersgegevens voor de PSO, en het privacybelang van de betrokken medewerker dat zich hiertegen verzet. Zowel uw eigen belang als belangen van derden kunnen hierbij worden meegewogen, zoals het belang van PSO-Nederland en het belang van de Nederlandse samenleving dat is gediend bij de PSO.

6.3 Aangezien voor gezondheidsgegevens een algemeen verwerkingsverbod geldt (zie punt 5 in het schema hierboven), kan verwerking van deze medewerkersgegevens niet worden gebaseerd op het gerechtvaardigd belang. Indien u medewerkersgegevens voor de PSO verwerkt voor één van de onderstaande PSO-doelgroepen, verwerkt u waarschijnlijk gezondheidsgegevens van bepaalde medewerkers.

Gezondheidsgegevens bij gebruik PSO	
Doelgroepen	• SW-geïndiceerd • WAO/WIA/WAZ • WAJONG • Jonggehandicapten die met een voorziening WML kunnen verdienen

6.4 Indien u voor de PSO:

6.4.1 Geen informatie opvraagt voor de bovenstaande doelgroepen, is er een reële kans dat u geen gezondheidsgegevens van uw medewerkers verwerkt. Indien dat het geval is, kunt u overwegen de medewerkers alleen te informeren over het verwerken van hun gegevens voor de PSO, en niet ook om hun toestemming te vragen.

6.4.2 Wel informatie opvraagt voor de bovenstaande doelgroepen, verwerkt u waarschijnlijk gezondheidsgegevens van bepaalde medewerkers en dient u zich te kunnen baseren op één van de wettelijke uitzonderingen op het verwerkingsverbod. Wellicht biedt de uitdrukkelijke toestemming van de medewerker hier uitkomst; zie hierna.

Uitdrukkelijke toestemming

6.5 Indien u voor het gebruik van de PSO gezondheidsgegevens van bepaalde medewerkers verwerkt, kunt u deze verwerking wellicht baseren op de uitdrukkelijke toestemming van de betrokken medewerkers. Een dergelijke toestemming vormt een uitzondering op het algemene verwerkingsverbod dat geldt voor het verwerken van bijzondere persoonsgegevens, waaronder gezondheidsgegevens.

6.6 Toestemming is alleen rechtsgeldig indien deze vrij, specifiek en geïnformeerd is gegeven. Zie hierover nader deze webpagina van de Autoriteit Persoonsgegevens. In de relatie tussen werkgevers en medewerkers kan discussie ontstaan of medewerkers hun toestemming in vrijheid hebben gegeven, gezien de gezagsverhouding tussen werkgevers en medewerkers.

6.7 Omdat u er belang bij heeft deel te nemen aan de PSO, kan zonder extra waarborgen onder de AVG ook voor de PSO discussie ontstaan over of de toestemming van de betrokken medewerkers rechtsgeldig is verkregen. Indien u uitdrukkelijke toestemming van uw medewerkers kiest als grondslag voor het verwerken van hun persoonsgegevens voor de PSO, is het daarom raadzaam goed te waarborgen dat zij hun toestemming in vrijheid kunnen geven of onthouden.

6.8 Om u praktische handvatten te geven, wordt in het volgende schema ter illustratie een aantal waarborgen voorgesteld. Let wel dat het implementeren van deze waarborgen geen garantie vormt dat u zich kunt beroepen op de toestemming van uw medewerkers. Dit zal namelijk steeds afhangen van de specifieke situatie waarin de toestemming is gegeven. Het is daarom raadzaam om goed te kijken naar hoe u in uw eigen organisatie zo veel mogelijk kunt waarborgen dat uw medewerkers hun toestemming in daadwerkelijke vrijheid kunnen geven.

Werkwijze vragen van uitdrukkelijke toestemming	
Aanwijzen één interne PSO-behandelaar	Door binnen uw organisatie één persoon aan te wijzen die gegevens over uw medewerkers verwerkt voor de PSO die mogelijkerwijs gezondheidsgegevens bevatten, wordt de verwerking hiervan beperkt tot het noodzakelijke. Daarnaast kan deze aangewezen persoon uw medewerkers om toestemming verzoeken voor het verwerken van hun persoonsgegevens – waaronder mogelijk ook gezondheidsgegevens – in het kader van de PSO. Indien met deze persoon een passende geheimhoudingsbepaling is overeengekomen (zie hieronder), kan in zekere mate worden gewaarborgd dat uw medewerkers rechtsgeldige toestemming kunnen verlenen.
Anonimiseren gezondheidsgegevens	Voordat inzage in de bewijsstukken aan de auditor wordt verleend, moeten deze zoveel mogelijk worden geanonimiseerd. Dit houdt in dat de stukken zo min mogelijk informatie moeten bevatten die herleidbaar is tot individuele medewerkers. Zo kunt u – waar mogelijk en in overleg met de auditor – zoveel mogelijk de volgende gegevens onleesbaar maken alvorens de stukken aan de auditor te openbaren: NAW-gegevens, personeelsnummer, functie, en de afdeling waar iemand werkt. Ook bij niet-schriftelijke gegevens, zoals interviews, moeten zo min mogelijk gegevens worden verstrekt die tot specifieke medewerkers herleidbaar zijn.
Geheim-houdings-clausules	Het is raadzaam dat zowel de aangewezen interne PSO-behandelaar als de auditor zijn gebonden aan een passende geheimhoudingsplicht met betrekking tot de gezondheidsgegevens van uw medewerkers. • Met de interne PSO-behandelaar kan dit contractueel worden vastgelegd in de arbeidsovereenkomst of in een aparte geheimhoudingsovereenkomst. • Met de auditor kan dit contractueel worden vastgelegd in de overeenkomst die u met hem aangaat.

7 Conclusie

Uit de informatie in deze handreiking blijkt dat indien de juiste waarborgen in acht worden genomen, de PSO in overeenstemming met de AVG kan worden gebruikt. Indien u nog verdere vragen heeft over privacy compliance bij de PSO of andere aspecten van de PSO, kunt u contact met ons opnemen via info@pso-nederland.nl.

*****