Protocol omgaan met vertrouwelijke informatie

VluchtelingenWerk Zuid-Nederland

Inhoudsopgave

1. Inleiding....3
2. Privacy principes en regels....4
   2.1 Missie van VluchtelingenWerk Zuid-Nederland....4
   2.2 Wet bescherming persoonsgegevens en andere wetten....4
   2.3 Doeleinden waarvoor VluchtelingenWerk Zuid-Nederland persoonsgegevens verwerken....4
   2.4 Toestemming van de cliënt als uitgangspunt....5
3. Transparantie en de rechten van een cliënt....5
   3.1 Algemeen....5
   3.2 Informatie aan een cliënt....5
   3.3 Recht op inzage, verbetering, aanvulling, verwijdering, afscherming, verzet en overdraagbaarheid....5
4. Omgang, beveiliging en bewaren van informatie....6
   4.1 Algemeen....6
      4.1.1. Verantwoordelijkheid....6
      4.1.2. Het Vluchtelingen Volg Systeem VVS....6
      4.1.3 Algemene en bijzondere persoonsgegevens....7
   4.2 Omgang met informatie....7
      4.2.1 Vertrouwelijke en niet-vertrouwelijke informatie-....7
      4.2.2. Toegang tot gegevens alleen op basis van noodzaak....7
      4.2.3. Zakelijke vastlegging en bewaartermijnen dossiers....8
      4.2.4 Geheimhoudingsplicht....9
   4.3 Praktische richtlijnen voor de omgang met informatie....9
      4.3.1. Begeleid altijd bezoekers....9
      4.3.2. Zorg voor een 'clear screen' en een 'clean desk'....9
      4.3.3. Raadpleeg, archiveer en vernietig informatie op de voorgeschreven wijze....10
      4.3.4. Bepaal op welke wijze en hoe je communiceert....10
      4.3.5. Thuiswerken of werken buiten een VluchtelingenWerk locatie....12
      4.3.6 Wees je bewust van het bespreken van informatie in een publieke ruimte of het openbaar vervoer....13
      4.3.7. Wees je bewust van het gebruik van (eigen) mobile devices....13
      4.3.8. Wees je bewust van het gebruik van externe opslagmedia....13
      4.3.9. Meld verlies van informatie altijd direct....14
      4.3.10. Wees je bewust van je plicht tot geheimhouding....14
      4.3.11. Rol ICT....14
      4.3.12. Proces rondom informatieverzoeken....14
      4.3.13. Handhaving....14
      4.3.14. Vragen of opmerkingen....14
   4.4 Beveiligingsmaatregelen....15
   4.5 Inbreuk op de beveiliging: de meldplicht datalekken....15
      4.5.1. Algemeen....15
      4.5.2. Interne meldprocedure en administratie....16
      4.5.3. Melden bij de Autoriteit Persoonsgegevens....17
      4.5.4. Melden bij cliënten....17
5. Informatie uitwisseling met andere organisaties....17

1 Inleiding

Binnen VluchtelingenWerk Zuid-Nederland gaan medewerkers[1] dagelijks om met vertrouwelijke informatie. Gegevens worden verzameld, digitaal vastgelegd of opgenomen in fysieke dossiers en indien noodzakelijk doorgegeven aan bepaalde instanties. Deze dagelijkse verwerking van vertrouwelijke gegevens betreft niet alleen persoonsgegevens van cliënten maar ook vertrouwelijke, privacy gevoelige, informatie en gegevens met betrekking tot de bedrijfsvoering van VluchtelingenWerk Zuid-Nederland
De Wet bescherming persoonsgegevens (afgekort Wbp) stelt strenge eisen aan de bescherming van persoonsgegevens. Het beleid van VluchtelingenWerk Zuid-Nederland voor de verwerking van de cliënt- en personeelsgegevens is hierop afgestemd. Regelgeving is opgesteld met als doel:

- bescherming tegen misbruik van gegevens;
- voorkomen dat gegevens die geregistreerd zijn voor een ander doel worden gebruikt dan waarvoor die registratie bedoeld is;
- de rechten van betrokkenen te waarborgen.

Sinds 1 januari 2016 is er in de Wbp een meldplicht datalekken opgenomen. De Autoriteit Persoonsgegevens heeft de mogelijkheid gekregen forse boetes op te leggen voor schending van de meldplicht en het niet op orde hebben van de informatiebeveiliging.

Dit protocol* geeft:

1. nadere uitleg over het omgaan met privacy gegevens bij VluchtelingenWerk Zuid-Nederland,
2. praktische richtlijnen voor de omgang met vertrouwelijke informatie
3. uitleg over de meldplicht datalekken en een beschrijving van de meldprocedure

Tot slot, het onderliggende protocol is voornamelijk geschreven met de verwerking van cliëntgegevens als uitgangspunt. Voor het verwerken van de persoonsgegevens van medewerkers van VluchtelingenWerk Zuid-Nederland gelden echter dezelfde strenge regels (beschreven in de Wbp). Onder andere de beschrijving van de meldplicht datalekken en de praktische richtlijnen zijn dus evenzeer van toepassing op de privacy van persoonsgegevens personeel.**

---

[1] Onder medewerkers worden zowel betaalde als onbetaalde medewerkers verstaan.

* Voor medewerkers van VluchtelingenWerk Zuid-Nederland is een aparte flyer met Do's en don'ts bij het omgaan met privacy gegevens beschikbaar. Deze geeft een uitwerking van de praktische richtlijnen.

** Voor vragen over het protocol, privacy van persoonsgegevens van cliënten en van personeel: neem in eerste instantie contact op met de leidinggevende en in tweede instantie met het bedrijfsbureau van VluchtelingenWerk Zuid-Nederland via het mailadres info-zuid@vluchtelingenwerk.nl

2 Privacy principes en regels

2.1 Missie van VluchtelingenWerk Zuid-Nederland

De Stichting heeft ten doel het zich op basis van de Universele Verklaring van de Rechten van de Mens in te zetten voor de bescherming van asielzoekers en vluchtelingen door persoonlijke steun en belangenbehartiging bij hun toelating opvang en maatschappelijke participatie in het werkgebied van de stichting en voorts al hetgeen met het vorenstaande rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord. De stichting zet zich daarnaast, op verzoek van gemeenten in haar werkgebied, in voor de begeleiding en ondersteuning van nieuwkomers.

VluchtelingenWerk Zuid-Nederland behartigt de belangen van vluchtelingen en helpt hen en andere nieuwkomers om een volwaardige plaats in onze samenleving te verwerven.

2.2 Wet bescherming persoonsgegevens en andere wetten

De Wbp stelt strenge eisen aan de bescherming van persoonsgegevens.
Persoonsgegevens zijn alle gegevens die betrekking hebben op een persoon.[2]
Persoonsgegevens mogen alleen voor vooraf vastgestelde doeleinden en op een zorgvuldige wijze verwerkt worden. Bij de verwerking van bijzondere persoonsgegevens moeten de belangen van betrokkenen (degenen van wie gegevens verwerkt worden) extra gewaarborgd worden. Bijzondere persoonsgegevens moeten daarom extra beveiligd en afgeschermd worden tegen oneigenlijk gebruik.
Naast de Wbp wordt ook de wetgeving omtrent rechtspositie, inburgering en participatie in acht genomen***.

2.3 Doeleinden waarvoor VluchtelingenWerk Zuid-Nederland persoonsgegevens verwerken

VluchtelingenWerk Zuid-Nederland heeft als doel optimale bescherming en ondersteuning te bieden aan cliënten tijdens de asielprocedure, vestiging, inburgering en participatie.
Om dit te kunnen bieden heeft VluchtelingenWerk Zuid-Nederland tijdens de verschillende soorten van begeleiding verschillende soorten persoonsgegevens nodig.

Uitwisseling van persoonsgegevens aan derden
Er wordt geen schriftelijke of mondelinge informatie aan andere personen, instanties of aan andere vluchtelingen / asielzoekers gegeven. Uitzonderingen daarop zijn:

- Als de cliënt uitdrukkelijke toestemming geeft voor informatie verstrekking
- Als het van levensbelang is voor de cliënt, zoals bij een dringende medische oorzaak.
- Het noodzakelijk is voor de uitvoering van een overeenkomst met VluchtelingenWerk Zuid-Nederland waarbij cliënt partij is (denk bijvoorbeeld aan de gegevensuitwisseling met DUO in het kader van de inburgering)
- Als het noodzakelijk is voor een wettelijke verplichting of gerechtvaardigd belang van VluchtelingenWerk Zuid-Nederland.

---

[2] Meer specifiek: alle gegevens die betrekking hebben op een geïdentificeerde of een identificeerbare natuurlijke persoon. (gegevens die betrekking hebben op een overleden persoon zijn in beginsel geen persoonsgegevens meer)

*** De Vreemdelingen wet, Wet inburgering, wetgeving in het kader van participatie en sociale zekerheid etc.

2.4 Toestemming van de cliënt als uitgangspunt

Persoonsgegevens van cliënten mogen alleen vastgelegd worden wanneer de cliënt daar uitdrukkelijke toestemming voor heeft gegeven en er een gerechtvaardigd doel is voor VluchtelingenWerk Zuid-Nederland om deze gegevens te verwerken.
Van uitdrukkelijke toestemming kan alleen sprake zijn als de cliënt voldoende uitleg heeft gekregen over welke gegevens vastgelegd worden door VluchtelingenWerk Zuid-Nederland, met welk doel deze gegevens worden verwerkt en aan welke derden deze gegevens verstrekt worden.

3 Transparantie en de rechten van een cliënt

3.1 Algemeen

Een belangrijk uitgangspunt in de wet is het *informationeel zelfbeschikkingsrecht.* Dat wil zeggen dat de cliënt het recht heeft om zelf te kunnen bepalen hoe met zijn of haar gegevens moet worden omgegaan. VluchtelingenWerk Zuid-Nederland zal dus steeds met individuele wensen rekening moeten houden. De cliënt moet daarom informatie krijgen waaruit blijkt welke gegevens, waarvoor, aan wie worden verstrekt en voor hoelang deze worden bewaard. VluchtelingenWerk Zuid-Nederland moet hierover transparant zijn en dit betekent dat cliënten uitvoerig worden geïnformeerd over wat wij met hun gegevens doen.

3.2 Informatie aan een cliënt

Het informeren van de cliënt gebeurt op de volgende manieren:
1. persoonlijk overhandigen van de folder *VluchtelingenWerk Zuid-Nederland en uw gegevens* aan de cliënt
2. mondelinge toelichting op de folder en op het formulier *Privacy en klachtrechtreglement.*
De korte uitleg over het formulier Privacy en klachtreglement, zoals deze als sjabloon beschikbaar is, kan hierbij als handvat dienen. In het geval de cliënt de Nederlandse taal nog onvoldoende beheerst is het zaak om met behulp van een tolk uitleg te geven

Na de bovenstaande uitleg wordt de cliënt gevraagd het machtigingsformulier te ondertekenen.
Tijdens de mondelinge toelichting dienen in ieder geval onderstaande onderwerpen met de cliënt besproken te worden:

3.3 Recht op inzage, verbetering, aanvulling, verwijdering, afscherming, verzet en overdraagbaarheid

De cliënt mag weten welke gegevens er zijn vastgelegd.
Een cliënt heeft altijd het recht om inzage te krijgen in zijn of haar dossier en te weten welke gegevens er zijn vastgelegd.

Rechten van de cliënt en zakelijke verslaglegging
Zoals hierboven al vermeld, heeft iedere cliënt het recht op inzage in zijn of haar dossier. Daarnaast heeft de cliënt het recht aan de medewerker te vragen om de geregistreerde informatie te wijzigen in de vorm van verbetering, aanvulling, verwijdering of afscherming van (gedeelten) uit het dossier.

Dit heeft consequenties voor de manier waarop in het dossier van de cliënt begeleidingsgegevens moeten worden vastgelegd. Aantekeningen in een dossier dienen zakelijk van aard te zijn. In de verslaglegging van het begeleidingstraject horen subjectieve, 'emotionele' opmerkingen niet thuis.

De cliënt kan een beroep doen op de klachtenregeling.
Iedere cliënt die niet tevreden is over de manier waarop VluchtelingenWerk Zuid-Nederland met zijn of haar gegevens omgaat, kan een klacht indienen. Een klacht kan ingediend worden en wordt behandeld volgens het klachtenreglement van VluchtelingenWerk Zuid-Nederland Dit reglement is te vinden in de kennismap van VluchtelingenWerk Zuid-Nederland, voor cliënten zijn er folders beschikbaar.

4 Omgang, beveiliging en bewaren van informatie

4.1 Algemeen

4.1.1. Verantwoordelijkheid

Wie is verantwoordelijk voor de zorgvuldige omgang met informatie?
Iedere medewerker van VluchtelingenWerk Zuid-Nederland heeft een eigen inlogaccount en heeft daarmee toegang tot de informatiesystemen van VluchtelingenWerk. Naast toegang tot digitaal verwerkte gegevens, krijgen medewerkers van VluchtelingenWerk Zuid-Nederland ook te maken met fysiek vastgelegde gegevens. Denk hierbij aan de fysieke cliëntdossiers op de diverse locaties van VluchtelingenWerk Zuid-Nederland.
Iedere medewerker van VluchtelingenWerk Zuid-Nederland, zowel betaald als onbetaald, is verantwoordelijk voor de zorgvuldige omgang met de informatie die beschikbaar is. Elke medewerker is daarnaast aan te merken als beheerder van de gegevens die hij of zij verwerkt (zowel fysiek als digitaal) in die zin dat de medewerker verantwoordelijk is voor de juistheid van de verwerkte gegevens en de juiste manier van verwerken hiervan.

4.1.2. Het Vluchtelingen Volg Systeem *VVS*

Binnen VluchtelingenWerk Zuid-Nederland hebben we te maken met veel gevoelige informatie over cliënten. De toegang tot persoonsgegevens wordt daarom zoveel mogelijk beperkt tot medewerkers die de gegevens nodig hebben om hun werk goed te kunnen uitvoeren. Het gaat hierbij met name om de VVS-dossiers, waar veel gevoelige en bijzondere persoonsgegevens in staan.
Op alle rapporten die uit VVS gegenereerd worden staat onderaan de verplichte risicoklasse vermeld. Deze risicoklassen lopen van 0 t/m 3.

- Vertrouwelijkheid klasse 0: 'publiek niveau'. Document bevat geen persoonsgegevens
- Vertrouwelijkheid klasse 1: 'basis niveau'. Document bevat beperkt aantal persoonsgegevens
- Vertrouwelijkheid klasse 2: 'verhoogd risico'. Document bevat gevoelige persoonsgegevens
- Vertrouwelijkheid klasse 3: 'hoog risico'. Document bevat bijzondere persoonsgegevens

4.1.3 Algemene en bijzondere persoonsgegevens

Het onderscheid tussen persoonsgegevens en bijzondere persoonsgegevens
Om een cliënt goed te kunnen begeleiden heeft VluchtelingenWerk Zuid-Nederland een aantal persoonsgegevens nodig om in het dossier van de cliënt vast te leggen. Dit betreft gegevens als: naam, adres en nationaliteit, maar ook gegevens over familie, persoonlijke omstandigheden en de asielprocedure. Naast deze 'gewone' persoonsgegevens kan het zijn dat er voor een goede begeleiding bijzondere persoonsgegevens vastgelegd moeten worden. Dit zijn bijvoorbeeld gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of geaardheid, of het lidmaatschap van een vakvereniging. Deze gegevens zijn voornamelijk van belang tijdens de juridische begeleiding op de centrale opvang (denk aan de vluchtverhaal analyse). In de dossiers worden alleen die gegevens bewaard die voor een goede begeleiding noodzakelijk zijn. Dat betekent dat bijvoorbeeld gegevens uit het vluchtverhaal niet meer van belang hoeven te zijn tijdens de maatschappelijke begeleiding en dus niet meer toegankelijk zijn voor medewerkers.

4.2 Omgang met informatie

4.2.1 Vertrouwelijke en niet-vertrouwelijke informatie-

Vertrouwelijke informatie betreft in ieder geval alle informatie en hiervan afgeleide data (op papier, digitaal of uit gesprekken) die aanwezig is over cliënten die zijn geregistreerd in of buiten het Vluchtelingenwerk Volg Systeem (VVS) en die (nog) niet openbaar is. Ook persoonsgegevens en gegevens over de bedrijfsvoering van de organisatie zijn vertrouwelijk. Vertrouwelijke gegevens zijn gegevens die niet anoniem zijn maar terug te herleiden tot personen zoals bijvoorbeeld: informatie van medewerkers (personeelsdossiers) en sollicitanten. Maar ook informatie over de stichting zoals gegevens over inkoop en de bedrijfsadministratie is vertrouwelijk.
Niet vertrouwelijke informatie is informatie die óf openbaar is óf waarvan het niet erg is als deze openbaar zou zijn. Een voorbeeld hiervan is het jaarverslag met die gegevens over de bedrijfsvoering en personen (medewerkers en cliënten) die openbaar beschikbaar zijn.

4.2.2. Toegang tot gegevens alleen op basis van noodzaak

Wie hebben er toegang tot de gegevens?
Een beperkt aantal medewerkers van VluchtelingenWerk Zuid-Nederland heeft toegang tot de dossiers van cliënten. In de regel zijn dit de medewerkers die direct betrokken zijn bij de begeleiding van de cliënt. Persoonsgegevens worden in principe niet uitgewisseld met derden tenzij er een noodzaak is om dit wel te doen. Denk bijvoorbeeld aan gegevensuitwisseling met het DUO (Dienst Uitvoering Onderwijs) in het kader van de inburgering, of gegevensuitwisseling met de gemeenten in het kader van de huisvestingstaakstelling.

Voor wie is informatie beschikbaar?
VluchtelingenWerk Zuid-Nederland hanteert het uitgangspunt dat gevoelige informatie alleen beschikbaar is voor medewerkers voor wie dat noodzakelijk is voor de uitoefening van hun functie of werkzaamheden. Dit is het 'need to know' principe. VluchtelingenWerk Zuid-Nederland hanteert daarom een autorisatiebeheer dat gekoppeld is aan de functie en/of de werkzaamheden van een medewerker.

4.2.3. Zakelijke vastlegging en bewaartermijnen dossiers

Bewaartermijnen van dossiers

Vanwege de bescherming van persoonsgegevens mogen gegevens niet langer bewaard worden dan noodzakelijk is. Dat geldt zeker voor vluchtelingen aangezien het vaak zal gaan om extra privacygevoelige informatie. Het is daarom van groot belang dat een deel van de gegevens op een zeker moment daadwerkelijk vernietigd wordt en een ander deel langer bewaard (zie onder bij Wettelijk kader.)

Verantwoordelijkheid voor VluchtelingenWerk Zuid-Nederland.

VluchtelingenWerk Zuid-Nederland mag (en soms moet) cliëntgegevens bewaren voor zover dit het begeleidings- of verantwoordingsdoel dient. Vanuit dit perspectief is de richtlijn dat als hiervan geen sprake meer is, de gegevens verwijderd worden. Praktisch gezien betekent dit dat zodra het begeleidingscontact met de cliënt duurzaam beëindigd is, het dossier afgesloten moet worden. Dit kan door het aan de cliënt mee te geven of, als dit niet mogelijk is, het dossier te vernietigen. Het digitale VVS dossier wordt dan gearchiveerd. Daarbij worden gevoelige persoonlijke gegevens geschoond. NAW- en trajectgegevens kunnen langer bewaard moeten worden in het kader van bijvoorbeeld de financiële verantwoording.

Wettelijk kader

Er zijn externe (wettelijke) criteria gesteld aan een bewaartermijn van 7 jaar vanuit juridisch perspectief (Burgerlijk Wetboek) en de belastingdienst. Vanuit administratief perspectief i.g.v. EU financiering, geldt een bewaartermijn van 10 jaar. Ook vanuit de eigen financiële administratie is er een bewaartermijn van 7 jaar vastgelegd. NB: er wordt gerekend met 7 jaar nadat de cliënt door VluchtelingenWerk is begeleid. Om te voldoen aan de administratieve bewaartermijnen hoeven nooit de contractbegeleidingsgegevens bewaard te worden.

Richtlijnen bewaartermijnen (samenvattend)

- Fysieke dossiers worden na beëindiging van de begeleidingsrelatie aan de cliënt meegegeven. Eigen aantekeningen èn niet meegenomen dossiers worden uiterlijk een jaar na het laatste contact met VluchtelingenWerk, vernietigd. Het digitale dossier in VVS wordt verhuisd naar het archief van VVS
- Het Landelijk Bureau zorgt voor de opschoning van de digitale gegevens in VVS indien blijkt dat een dossier 2 jaar inactief is. Hierbij wordt de volgende procedure gehanteerd:
    - Het dossier wordt opgeschoond qua begeleidingsgegevens volgens een landelijk opgesteld opschoningsprotocol
    - Het digitale dossier wordt opgehaald voor centrale archivering (in het landelijk VVS archief)
    - Het geschoonde VVS dossier is daarna (in het landelijk VVS archief) nog 5 jaar opvraagbaar voor regionale stichtingen
    - Na 7 jaar (i.g.v. EU financiering geldt 10 jaar) niet gebruikt te zijn wordt het digitale VVS dossier vanuit het centrale archief definitief verwijderd.

4.2.4 Geheimhoudingsplicht

Alle medewerkers zijn gebonden aan een geheimhoudingsplicht.
Elke medewerker van de stichting heeft een geheimhoudingsplicht die voortvloeit uit onderschrijving (ondertekenen van een medewerkersovereenkomst) van de gedragscode. Dit betekent dat er niet met mensen buiten de stichting over zaken mag worden gesproken die aan een medewerker zijn toevertrouwd tijdens de werkzaamheden voor VluchtelingenWerk Zuid-Nederland. Deze geheimhoudingsplicht geldt ook nadrukkelijk ná beëindiging van de werkzaamheden voor VluchtelingenWerk Zuid-Nederland.
Met betrekking tot de privacy van cliënten betekent dit:

- In externe contacten staat het belang van de cliënt voorop.
- In externe contacten wordt er naar gestreefd het imago van cliënten van de stichting positief te beïnvloeden en in geval van de media uitdrukkelijk de belangen van betreffende cliënt te behartigen.

4.3 Praktische richtlijnen voor de omgang met informatie

4.3.1. Begeleid altijd bezoekers

Regelmatig worden externen uitgenodigd op een VluchtelingenWerk locatie. Zorg ervoor dat bezoekers altijd worden opgehaald bij de receptie en na afloop van de afspraak weer naar de uitgang worden begeleid. Dit geldt ook voor het ontvangen van oud-medewerkers of medewerkers van andere organisaties.

4.3.2. Zorg voor een 'clear screen' en een 'clean desk'

In bepaalde situaties hebben ook derden toegang tot een locatie van VluchtelingenWerk. Ruim daarom bij het verlaten van je werkplek vertrouwelijke en overige gevoelige cliënt-informatie of organisatie-informatie altijd op. Dit kan je vaste werkplek betreffen, maar ook een tijdelijke vergaderruimte, flexplek of projectruimte. Ladeblokken en archiefkasten zijn voorzien van een slot. Gebruik deze indien nodig.

Bij een clean desk-beleid hoort ook dat je al je prints uit het kopieerapparaat haalt. Houd de tijd tussen afdrukken en het daadwerkelijk ophalen bij de printer zo kort mogelijk. Vind je documenten van collega's bij het kopieerapparaat, laat deze dan niet onbeheerd achter en geef deze persoonlijk aan de betreffende collega of gooi ze in de bak voor papiervernietiging.

Aandachtspunten bij het veilig houden van je werkplek:

- Vergrendel altijd je computer als je je werkplek verlaat. Dit kan eenvoudig door linksonder te klikken en het commando "Sessie vergrendelen" aan te klikken
- Schakel je computer altijd uit op het moment dat je naar huis gaat, berg een eventuele laptop op in een daarvoor bestemd kluisje of afsluitbare kast.
- Je inloggegevens (username en password) zijn strikt persoonlijk. Geef deze dan ook nooit prijs aan een ander, maar bewaar ze uitsluitend voor jezelf. Berg je inloggegevens zorgvuldig op en laat deze niet achter op je bureau of op je computer.
- Vergeet bij het verlaten van je werkplek/vergaderruimte niet om de whiteboards schoon te vegen of de flip-over vellen te vernietigen. Namen van cliënten of andere persoonsgegevens en vertrouwelijke informatie dienen altijd te worden verwijderd.

4.3.3. Raadpleeg, archiveer en vernietig informatie op de voorgeschreven wijze

Bij de meeste werkzaamheden binnen VluchtelingenWerk Zuid-Nederland is het digitale dossier leidend. Het is dan ook belangrijk dat alle relevante fysieke en digitale gegevens tijdig en juist worden toegevoegd aan de digitale werkomgeving van VluchtelingenWerk of aan het VVS.

Ontvangen e-mails en gemaakte brieven, memo's en rapporten dien je zelf toe te voegen aan de digitale werkomgeving of aan het VVS. Houd hierbij rekening met VluchtelingenWerk richtlijnen omtrent Dossiervorming.

- Maak voor het opbergen van fysieke documenten altijd gebruik van de daarvoor bestemde archiefkasten of kluizen. Het vernietigen van documenten geschiedt via de daarvoor bestemde papiercontainers, de papiervernietigers of de bedrijven die vertrouwelijke papieren ter vernietiging komen ophalen op uw locatie. Zorg dan ook tot het moment van ophalen voor een data zekere opslag. Rondslingerende gevoelige gegevens die door een onbevoegde wordt ingezien betekent dat er sprake is van een meldplichtig datalek.
- Archiveer dossiermappen. Zorg ervoor dat bij het aanbieden van dossiers en documenten voor fysieke archivering kritisch is gekeken naar de inhoud en volledigheid. Schaduw- of werkdossiers, kopieën, enzovoorts maken het liefst geen deel uit van het archief.
- Persoonsgegevens die voorkomen in archiefbescheiden moeten tegelijk met de archiefbescheiden waarvan ze deel uitmaken worden vernietigd. Persoonsgegevens die niet behoren tot de archiefbescheiden moeten verwijderd worden zodra de gegevens niet meer noodzakelijk zijn voor het doel waarvoor de gegevens zijn verkregen of worden verwerkt.

4.3.4. Bepaal op welke wijze en hoe je communiceert

Per gewone post

Brieven en andere poststukken kunnen zowel regulier als aangetekend worden verstuurd. Met regulier wordt hier bedoeld dat brieven via de standaard postprocedure dagelijks worden verzonden. Specifieke afspraken en werkwijzen over het aanleveren van brieven verschilt per locatie. Vraag de werkwijze op jouw locatie na.

- Laat gevoelige informatie niet open en bloot liggen in de postvakken, maar stop deze in een gesloten envelop.
- Richtlijn voor externe post is dat het verstrekken van gevoelige (persoons)gegevens aangetekend gebeurt.
- Maak je geen gebruik van een VluchtelingenWerk-retourenvelop, geef dan – in geval van persoonsgevoelige informatie – altijd duidelijk het retouradres weer in de brief en op de envelop/omslag.

Via de telefoon
Wees ook via de telefoon terughoudend met het bespreken van vertrouwelijke informatie. Zeker als je niet zeker weet wie je aan de lijn hebt. Verifieer zo nodig het telefoonnummer. Dit kan door de betreffende beller terug te bellen en/of het telefoonnummer te verifiëren via de telefoongids.nl of een zoekmachine.

- Houd er bij het inspreken van een voicemail bericht rekening mee dat iemand anders de boodschap zou kunnen horen. Spreek persoonlijke berichten niet in als derden kunnen meeluisteren en volsta waar mogelijk met de mededeling dat je teruggebeld wilt worden over een bepaald onderwerp.
- Je kunt je voicemail daarnaast voorzien van een wachtwoord. Vertrouwelijke berichten kunnen dan niet zomaar via een ander toestel worden beluisterd.

Per (elektronische)fax
Bij het gebruik van de fax spelen ook risico´s. De afzender heeft namelijk weinig controle op het ontvangstproces. Je weet niet altijd wie de fax in ontvangst neemt of dat de fax wel of niet in een beveiligde omgeving wordt bewaard. Verstandig is om vooraf te telefoneren met de ontvanger om te voorkomen dat er een datalek kan ontstaan. Een ander risico is de foutgevoeligheid bij het intoetsen van het faxnummer.

Via internet
Alle medewerkers van VluchtelingenWerk Zuid-Nederland hebben op hun werkplek toegang tot het internet. Het gebruik van internet op je werkplek is beperkt beschikbaar voor privédoeleinden: voor zover je werkzaamheden of je collega´s hiervan geen hinder ondervinden.

- Wees je bewust van de risico’s bij het gebruik van het internet, met name bij het plaatsen van berichten in combinatie met je geheimhoudingsplicht. Denk hierbij bijvoorbeeld aan het gebruik van social media. Het volledig verwijderen van geplaatste informatie van internet is zeer moeilijk, zo niet onmogelijk.

Via e-mail
Een medewerker mag niet zomaar de e-mailbox van een andere medewerker bekijken. Een eventueel door de medewerker aangewezen vertrouwenspersoon is de eerste in lijn die toestemming heeft. In bepaalde gevallen -en onder strikte voorwaarden- kan de ICT Servicedesk toegang verschaffen aan een speciaal daarvoor aangewezen collega.

- In principe kan een collega of leidinggevende alleen inzage krijgen in de e-mailbox als de medewerker hiervoor zelf toestemming heeft gegeven (door een collega als vertegenwoordiger aan te wijzen, of door uitdrukkelijk toestemming te geven, bijvoorbeeld per e-mail).
- Slechts in bijzondere of uitzonderlijke gevallen kan de leidinggevende goedkeuring geven voor het doorzoeken van de mailbox door iemand anders: als het niet mogelijk is om de medewerker te bereiken om toestemming te vragen (bijvoorbeeld bij langdurig ziekenhuisverblijf, ontslag op staande voet e.d.) en het betreffende document noodzakelijk is om lopende werkzaamheden voort te zetten of af te ronden.
- Het opzoeken van het gevraagde document gebeurt dus in beginsel door een door de medewerker aangewezen vertrouwenspersoon.

- Mocht dit niet mogelijk zijn, kan de directeur iemand anders aanwijzen om de bestanden te zoeken. Bij voorkeur de leidinggevende van de medewerker. Eventueel kan een derde persoon worden gevraagd om mee te kijken om te verifiëren dat de privacy voldoende wordt gewaarborgd.
- Mocht dit niet mogelijk zijn, kan de directeur toestemming geven aan de regionale ICT-functionaris om de documenten in de mailbox te zoeken. De ICT-afdeling heeft toegang tot alle mailboxen en accountinformatie, mocht het nodig zijn. Dit dient schriftelijk aangevraagd en afgehandeld te worden via een formeel en schriftelijk verzoek, naar de ICT Servicedesk.
- Als het om een document gaat waarvoor niet ver gezocht hoeft te worden in de e-mailbox, zal er vanuit privacy-oogpunt veelal geen bezwaar zijn om dit document uit de mailbox te halen. Hoe meer er in de e-mailbox gezocht moet worden en hoe meer e-mails geopend moeten worden om het document te vinden, hoe zwaarder het belang van de betreffende medewerker zal wegen en hoe eerder persoonlijke toestemming van de medewerker of diens vertrouwenspersoon benodigd is.

4.3.5. Thuiswerken of werken buiten een VluchtelingenWerk locatie

VluchtelingenWerk faciliteert medewerkers die thuis of elders willen werken. Dit is voor zover de aard van de functie dit toelaat. Veel van de toepassingen die worden gebruikt (Zimbra, VVS, Intranet, Vluchtweb) zijn zogenaamde web-applicaties. Dat betekent dat ze met de juiste gebruikersnaam en wachtwoord (en voor VVS: met token) via iedere computer met internetverbinding zijn te benaderen.
Daarnaast is er voor een aantal functies een beveiligd ICT-netwerk beschikbaar naar de bestanden op de eigen servers.
Wanneer je buiten een VluchtelingenWerk-locatie werkt, ga dan net zo zorgvuldig met (vertrouwelijke) informatie om als op locatie.
Voor thuis/elders-werken gelden, in aanvulling op de uitgangspunten genoemd onder punt 2 (clean desk), de volgende aandachtspunten:

- De informatie is niet voor je huisgenoten, partner, vrienden of welke andere onbevoegden dan ook bestemd. Wees je dus bewust van de risico's op onbevoegde raadpleging door derden en het ontstaan van een meldplichtig datalek.
- Kopieer geen informatie vanuit het VluchtelingenWerk-netwerk naar je persoonlijke computer, mobile device of andere datadragers, mocht dit al mogelijk zijn.
- Wees terughoudend met het printen van informatie tijdens het thuis/elders-werken en bewaar de geprinte gegevens na gebruik niet buiten een VluchtelingenWerk-locatie. Neem altijd je documenten mee (terug) naar de locatie en vernietig deze in de daarvoor bestemde afgeschermde papierbakken.
- Gooi nooit vertrouwelijke informatie bij je reguliere afval weg om te voorkomen dat er een meldplichtig datalek ontstaat. Houd bij het vervangen van je thuisprinter of computer ook rekening met het feit dat sommige apparaten over een geheugenkaart beschikken dat inzicht geeft in verrichte printopdrachten.
- Wees alert op je omgeving wanneer je buiten kantoor telefoneert. Voorkom dat onbevoegden kunnen meeluisteren met vertrouwelijke gesprekken.

Het is alleen toegestaan om vertrouwelijke informatie (in hard copy) mee te nemen als dit noodzakelijk is voor de uitvoering van je werkzaamheden. Denk bijvoorbeeld aan het bezoeken van een cliënt of het verhuizen van het fysieke dossier naar een andere locatie. In die gevallen, waarbij informatie buiten een VluchtelingenWerk-locatie wordt meegenomen, dient uiteraard de grootste zorgvuldigheid te worden betracht. Heb je twijfels of je bepaalde informatie wel of niet mag meenemen, bespreek dit dan van tevoren met je leidinggevende.

Het meenemen van vertrouwelijke gegevens en deze vervolgens onbeheerd in je auto of in het openbaar vervoer achterlaten, wordt aangemerkt als onzorgvuldig. Dit geldt zowel voor fysieke als ook voor digitale gegevens.

4.3.6 Wees je bewust van het bespreken van informatie in een publieke ruimte of het openbaar vervoer

Wees terughoudend met het bespreken van informatie met collega's of derden in een publieke ruimte of het openbaar vervoer. Dit om te voorkomen dat iemand anders mee luistert. Dat geldt natuurlijk ook als je documenten of e-mails leest.

4.3.7. Wees je bewust van het gebruik van (eigen) mobile devices[3]

Wellicht maak je tijdens je werk ook gebruik van een laptop of ander mobile devices, zoals een tablet. Neem ze uit veiligheidsoverwegingen alleen mee als dat nodig is voor je werk.

- Het gebruik van mobile devices brengt een aantal specifieke beveiligingsrisico's met zich mee. Niet alleen kunnen virussen e.d. gemakkelijker tot het apparaat doordringen (bijvoorbeeld via randapparatuur die wordt aangesloten of via het gebruik van usb-sticks). Zolang er geen aansluiting met het VluchtelingenWerk-netwerk wordt gezocht, wordt er geen back-up van bestanden gemaakt.
- Een mobile device kan persoonlijke informatie bevatten, zoals adresgegevens, berichten, korte notities en voicemailberichten. Telefoons, laptops en tablets zijn bovendien diefstalgevoelige apparaten. Bij verlies liggen deze gegevens op straat en kan er sprake zijn van een meldplichtig datalek. Voorzie het mobile device daarom altijd van een pincode (gebruik geen standaardinstellingen als 0000 of 1234).
- Verder geldt: hoe minder informatie er op het apparaat aanwezig is, hoe minder er per ongeluk op straat kan belanden. Verwijder oude teksten, berichten en gegevens daarom zoveel mogelijk. Verlies van het mobile device betekent niet alleen verlies van de informatie; VluchtelingenWerk kan ook hoge boetes krijgen als dat gebeurt.
- Vanzelfsprekend neem je uiterste zorgvuldigheid in acht bij het meenemen van een mobile device om diefstal of verlies hiervan te voorkomen. Een mobile device meenemen en achterlaten in bijvoorbeeld een auto of café wordt door VluchtelingenWerk aangemerkt als onzorgvuldig handelen.

4.3.8. Wees je bewust van het gebruik van externe opslagmedia

Met gebruik van externe opslagmedia (bijvoorbeeld Dropbox, Google of WeTransfer e.d.) wordt informatie buiten de bescherming van de beheerde omgeving gebracht. Daarmee wordt die informatie buiten alle beveiligingsmaatregelen van VluchtelingenWerk gebracht, wat de risico's sterk verhoogt.

- Breng bestanden dan ook zo snel mogelijk over naar de netwerkomgeving van VluchtelingenWerk, zodat toegang voor (bevoegde) anderen, bescherming en bewaring (back up) en opschoningsprocedures goed zijn geregeld. De ICT Servicedesk kan je eventueel hierbij helpen.
- Gebruik externe opslagmedia alleen wanneer dit strikt noodzakelijk is en voorzie de data waar mogelijk van een wachtwoord.

[3] Zoals laptops, smartphones, USB sticks, tablets, e-readers e.d.

4.3.9. Meld verlies van informatie altijd direct
Mocht het voorkomen dat je (vertrouwelijke) informatie verliest, meld dat dan onmiddellijk bij je leidinggevende. Je leidinggevende bepaalt vervolgens de ernst van de zaak en adviseert je over de te nemen vervolgstappen. Mocht er sprake kunnen zijn van een meldplicht datalek dan dient dit door VluchtelingenWerk binnen 72 uur na ontdekking te worden gemeld bij de Autoriteit Persoonsgegevens op straffe van een forse boete (zie ook punt 11 en 4.5.2.). De termijnen zijn dus kort! Verlies van hardware (laptop, smartphone, tablet) is altijd verlies van (vertrouwelijke) informatie.

4.3.10. Wees je bewust van je plicht tot geheimhouding
Op iedere medewerker van VluchtelingenWerk rust een geheimhoudingsplicht. Hier heb je ook voor getekend. Het bespreken van vertrouwelijke informatie met derden is dan ook verboden en kan zelfs strafbaar zijn.[4] Twijfel je of je informatie met een collega of een derde mag delen, vraag het dan na bij je leidinggevende. In uiterst bijzondere gevallen is het delen van informatie weer verplicht (zie Gedragscode VluchtelingenWerk Nederland).

4.3.11. Rol ICT
De ICT Servicedesk is bevoegd om bij noodsituaties toegang te krijgen tot data en middelen. De namen van leidinggevenden en vertrouwenspersonen van alle locaties zijn bij de landelijke ICT Servicedesk bekend.

4.3.12. Proces rondom informatieverzoeken
Iedereen binnen VluchtelingenWerk Zuid-Nederland kan een vertrouwenspersoon voor zijn of haar account aanwijzen en doorgeven aan zijn leidinggevende. In noodsituaties (ziekte, onbereikbaarheid, et cetera) kan een gemotiveerd inzageverzoek worden gericht aan de vertrouwenspersoon. Mocht dit niet mogelijk zijn dan kan de leidinggevende toestemming geven aan de regionale of landelijke ICT Servicedesk om het inzageverzoek in behandeling te nemen.

4.3.13. Handhaving
Van een VluchtelingenWerk-medewerker wordt verwacht dat hij of zij zorgvuldig omgaat met (vertrouwelijke) informatie en de organisatiemiddelen die hij of zij op basis van zijn of haar werkzaamheden tot zijn of haar beschikking heeft. Het (opzettelijk) onzorgvuldig omgaan met informatie of organisatiemiddelen kan de medewerker dan ook (ernstig) worden aangerekend. De ernst wordt hierbij onder meer gewogen op basis van de mate van opzet, de mate van onzorgvuldigheid, de recidive en/of de ontstane gevolgen. De data en middelen blijven altijd eigendom van VluchtelingenWerk Zuid-Nederland.

4.3.14. Vragen of opmerkingen
Voor al je vragen en/ of opmerkingen over de inhoud en werking van deze richtlijn, kun je terecht bij je leidinggevende.

[4] Artikel 272 Wetboek van Strafrecht: Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

4.4 Beveiligingsmaatregelen

Technische/organisatorische beveiliging digitale dossiers (VVS)

- De leidinggevende bepaalt welke medewerkers toegang krijgen tot het VluchtelingenVolgSysteem (VVS). Een medewerker kan alleen inloggen als hij of zij persoonlijke inloggegevens heeft gekregen (gebruikersnaam en wachtwoord). Daarenboven kan alleen ingelogd worden met een persoonlijk token (apparaat dat unieke 'token-codes' genereert) dat gekoppeld is aan voornoemde inloggegevens.
- Elke medewerker krijgt toegang tot VVS op grond van een bepaald functieprofiel. Het functieprofiel bepaald welke dossiers de medewerker mag zien en/of bewerken en welke gegevens de medewerker mag zien en/of bewerken. In de regel heeft een medewerker alleen toegang tot de dossiers waarbij hij of zij direct betrokken is in het kader van de begeleiding. Ook heeft deze medewerker toegang tot uitsluitend het soort informatie die direct van belang is voor de betreffende begeleiding.

Technische/organisatorische beveiliging fysieke dossiers

- Fysieke dossier worden bewaard in dossier(laden)kasten die afgesloten kunnen worden. Deze kasten staan in de spreekuurruimte of in de kantoor/archiefruimte en niet in de wachtruimte. (n.b. cliënten hebben geen toegang tot dit archief en dienen niet alleen gelaten te worden terwijl de dossierkasten niet zijn afgesloten)
- Indien de ruimte gedeeld wordt met een andere instelling worden er afspraken gemaakt met hen over het afsluiten van dossierkasten.
- De ruimte waarin het archief met dossierkasten zich bevindt moet eveneens afgesloten kunnen worden.
- Medewerkers dienen afspraken te maken over de plaats waar de sleutels bewaard worden. Deze sleutels worden alleen afgegeven aan medewerkers van de Stichting. Vanwege de privacy zijn kasten altijd op slot als er zich geen medewerkers bevinden in betreffende ruimte, evenals buiten kantoortijden.
- Dossiers dienen niet door medewerkers mee naar huis te worden genomen.

4.5 Inbreuk op de beveiliging: de meldplicht datalekken

4.5.1. Algemeen

Dit protocol is er met name op gericht om te voorkomen dat vertrouwelijke persoonsgegevens ongewenst 'op straat komen te liggen' of dat persoonsgegevens op de verkeerde manier worden verwerkt. In paragraaf 4.3 zijn praktische richtlijnen opgenomen voor het omgaan met vertrouwelijke informatie en worden de risico's benoemd wanneer zich een zogenoemd datalek voordoet.
Een datalek is elke inbreuk op de beveiliging 'die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'.
Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens. Voorbeelden van datalekken zijn: een kwijtgeraakt cliëntdossier, een gestolen laptop met hierop cliëntgegevens of 'rondslingerende' rapportages uit VVS met hierop persoonsgegevens.

Mocht er, ondanks alle maatregelen, toch sprake zijn van een datalek dan dient dit door VluchtelingenWerk..... binnen 72 uur na constatering te worden gemeld bij de Autoriteit Persoonsgegevens. Om te kunnen voldoen aan deze korte termijn moet bij constatering van een datalek onderstaande procedure worden gevolgd.

4.5.2. Interne meldprocedure en administratie

Interne meldprocedure

1. Iedere onbetaalde medewerker die een datalek heeft geconstateerd, moet dit onverwijld melden bij zijn of haar direct leidinggevende. Vermeld zoveel mogelijk details over het datalek en geef aan waarom dit een inbreuk is op de beveiliging en welke (ernstige) gevolgen dit kan hebben voor de betrokkene.
2. De betaald medewerker (leidinggevende) die een melding heeft gekregen van zijn of haar medewerker over een mogelijk datalek moet de melding direct beoordelen. Als er kans is op gevolgen voor de betrokkene dan moet er direct een melding gedaan worden bij het interne meldpunt datalekken door een email te sturen naar melden-datalek@vluchtelingenwerk.nl. Vermeld zoveel mogelijk details over het datalek en geef aan waarom dit een inbreuk is op de beveiliging en welke (ernstige) gevolgen dit kan hebben voor de betrokkene. De email moet tevens als cc verstuurd worden naar de direct leidinggevende. De betaald medewerker die zelf een datalek constateert moet op dezelfde manier een melding doen via melden-datalek@vluchtelingenwerk.nl (inclusief een cc naar zijn of haar direct leidinggevende).
3. De leidinggevende die in cc is geïnformeerd over een melding bij het interne meldpunt datalekken, beoordeelt samen met de betaald medewerker de ernst van het datalek. Met name wordt er gekeken welke (ernstige) gevolgen het datalek kan hebben voor de betrokkene. Als het waarschijnlijk is dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene dan wordt de verantwoordelijke (directeur-bestuurder) onmiddellijk hierover geïnformeerd.
4. Nadat de verantwoordelijke is geïnformeerd over een datalek met mogelijk ernstige gevolgen voor de betrokkene, beslist de verantwoordelijke om de betrokkene hier al dan niet over te informeren. Wanneer de verantwoordelijke beslist om de betrokkene te informeren, omvat de kennisgeving in ieder geval de aard van de inbreuk, de instanties waar meer informatie over de inbreuk kan worden verkregen en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.

Administratie m.b.t. melding datalekken

Op het moment dat er een melding heeft plaatsgevonden bij het meldpunt datalekken (melden-datalek@vluchtelingenwerk.nl) geldt in alle gevallen dat alle verdere correspondentie inzake melding, behandeling en afhandeling bewaard moet worden. Dit betekent in de praktijk dat correspondentie inzake meldingen in alle gevallen moet worden doorgegeven aan de secretaris van VluchtelingenWerk Zuid-Nederland die namens de stichting de bewaarplicht uitvoert.

4.5.3. Melden bij de Autoriteit Persoonsgegevens

De onderstaande meldprocedure wordt gevolgd bij datalekken

1. Elke melding die wordt gedaan bij het meldpunt datalekken (melden-datalek@vluchtelingenwerk.nl), wordt op het Landelijk Bureau inhoudelijk en technisch beoordeeld. De beoordeling vindt mede plaats aan de hand van de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens.
2. Wanneer op het Landelijk Bureau wordt beoordeeld dat de melding serieus is, wordt dit gemeld aan de directeur-bestuurder van VluchtelingenWerk Zuid-Nederland en de juridisch adviseur van de landelijke Vereniging. Afhankelijk van de melding kan er ook door gemeld worden aan een aantal regionale directeuren, als het een regio overstijgend probleem is of aan de landelijke directeur als het een landelijk probleem is.
3. De directeur-bestuurder van VluchtelingenWerk Zuid-Nederland is verantwoordelijke en besluit of er een melding van het datalek gedaan wordt bij de Autoriteit Persoonsgegevens. Om tot dit oordeel te komen overlegt de directeur-bestuurder met de juridisch adviseur van VluchtelingenWerk Nederland inzake de privacywetgeving.

De melding van het datalek aan de Autoriteit Persoonsgegevens omvat in ieder geval de aard van de inbreuk, een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die zijn getroffen of worden voorgesteld te treffen om deze gevolgen te verhelpen.

4.5.4. Melden bij cliënten

Een datalek moet bij clienten worden gemeld als de persoonsgegevens die getroffen zijn door het datalek, niet goed genoeg beveiligd zijn om onbevoegde raadpleging te voorkomen. Bovendien moet het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene. Melding aan de client kan achterwege worden gelaten als hiervoor zwaarwegende redenen zijn.

5 Informatie uitwisseling met andere organisaties

Doelbinding, transparantie, grondslag en verenigbaar gebruik

Voor VluchtelingenWerk Zuid-Nederland is het vaak noodzakelijk om gegevens van cliënten te delen met andere organisaties zoals met de ketenpartners IND en COA. Maar ook met gemachtigden, gemeenten, opleidingsinstellingen etcetera. Dergelijke gegevensuitwisselingen mogen alleen gebruikt worden voor de doelen waarvoor de gegevens van een cliënt verkregen zijn of voor doelen die daarmee verenigbaar zijn. De belangrijkste grondslagen voor gegevensuitwisselingen zijn: de toestemming van cliënt, de uitvoering van de overeenkomst met de cliënt (denk bijvoorbeeld aan de uitwisseling met inburgeringsopleidingen) of de naleving van een wettelijk voorschrift (denk bijvoorbeeld aan de uitwisseling met gemeenten).

Voor uitwisselingen met andere organisaties geldt dat hiervoor altijd de vertrouwelijkheid in acht wordt genomen en dat alleen gegevens worden uitgewisseld die noodzakelijk zijn voor de gestelde doelen. Uitwisselingen mogen alleen worden uitgevoerd als vooraf duidelijk is op basis van welke gerechtvaardigde grondslag en voor welk gerechtvaardigd doeleinde gegevens moeten worden gedeeld. Ook moet vooraf duidelijk zijn welke persoonsgegevens minimaal nodig zijn om te delen. Meer dan wat nodig is mag niet worden gedeeld met andere organisaties!