WIL Werk en Inkomen Lekstroom

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 2237

22 november 2024

Officiële uitgave van de gemeenschappelijke regeling Werk en Inkomen Lekstroom

Intern privacybeleid Werk en Inkomen Lekstroom

Inleiding

Dit nieuwe interne privacybeleid vervangt alle voorgaande beleidsdocumenten met vergelijkbare inhoud. Na onderzoek is gebleken dat het vorige interne privacybeleid te weinig informatie bevatte en onvolledig was. Daarom is er binnen Werk en Inkomen Lekstroom (hierna te noemen: '**WIL**') de behoefte ontstaan aan dit nieuwe interne privacybeleid.

Dit intern privacybeleid fungeert als een leidraad voor hoe we binnen WIL omgaan met privacygevoelige gegevens, zogeheten persoonsgegevens. Wij willen graag zorgvuldig omgaan met de persoonsgegevens van onze cliënten, websitebezoekers, partners, medewerkers, sollicitanten en andere personen.

Het is als medewerker belangrijk om het privacybeleid na te leven. Privacy en betrouwbaarheid staan bij WIL hoog in het vaandel. Door als organisatie dit privacybeleid na te leven, wordt de privacy van alle personen van wie de persoonsgegevens door WIL worden verwerkt, gewaarborgd. Voor het op een juiste manier verwerken van persoonsgegevens is het belangrijk dat ieder zijn of haar verantwoordelijkheid daarin neemt. Met het beschrijven van de maatregelen in dit privacybeleid neemt WIL haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving waaronder de Algemene verordening gegevensbescherming (hierna te noemen: '**AVG**').

In dit privacybeleid wordt onder andere uitgelegd wat persoonsgegevens zijn, welke regels er gelden bij het gebruik van deze persoonsgegevens en welke maatregelen wij nemen bij het gebruik van deze persoonsgegevens. Als medewerker dien je deze informatie door te nemen. Heb je behoefte aan specifieke informatie over het delen van persoonsgegevens met externe organisaties? Kijk dan naar Bijlage 1 bij dit beleid. Daar vind je namelijk hoe we daarmee omgaan.

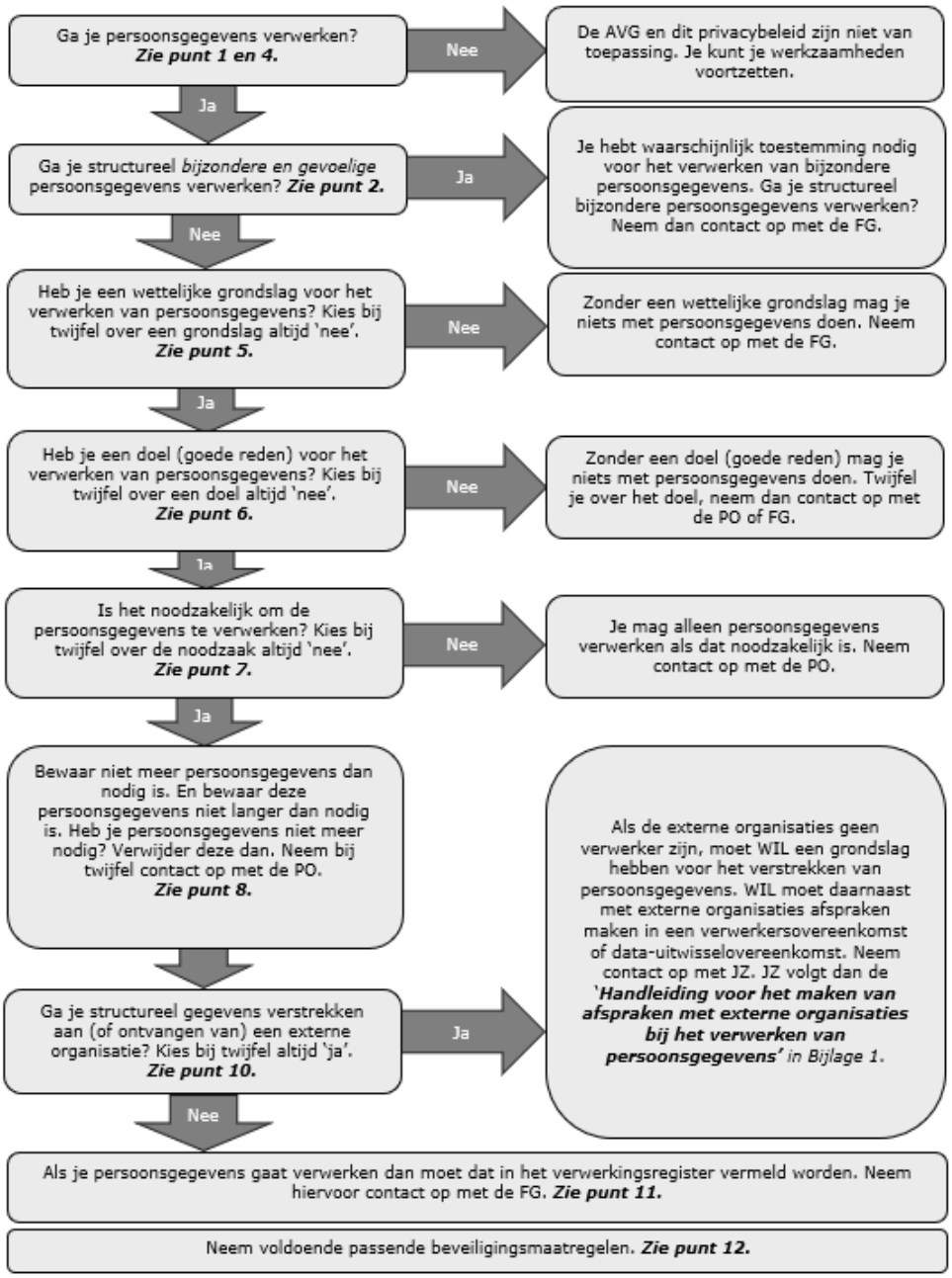
Als je vragen hebt over dit privacybeleid, als je een datalek wil melden, als een betrokkene verzoekt om zijn rechten uit te oefenen of als je algemene vragen hebt met betrekking tot privacy, dan kan je terecht bij de Privacy Officer ('PO') van WIL. Met betrekking tot privacyvragen is de PO het eerste aanspreekpunt. De PO is bereikbaar via het mailadres: privacy@wil-lekstroom.nl.

Met vragen over privacygerelateerde zaken kun je ook terecht bij de functionaris gegevensbescherming ('**FG**'). Met betrekking tot sommige zaken moet de FG altijd worden aangehaakt, bijvoorbeeld als je structureel bijzondere of gevoelige persoonsgegevens wilt verwerken, als je persoonsgegevens uit verschillende databases wilt combineren, er hoge risico's zijn bij een verwerking, je een data protection impact assessment ("**DPIA**") wilt uitvoeren of in dit privacybeleid naar de FG wordt doorverwezen. Je kunt de FG bereiken via het mailadres: FG@wil-lekstroom.nl.

Dit privacybeleid is voor het laatst aangepast op 11 oktober 2024. Houd er rekening mee dat dit privacybeleid en de bijbehorende regelgeving constant in ontwikkeling zijn. Als het privacybeleid wijzigt, stellen we je daarvan op de hoogte.

Stappenplan | Verwerken van persoonsgegevens

Verwerk je persoonsgegevens of ga je in de toekomst persoonsgegevens verwerken? Volg dan dit stappenplan.



Privacybeleid | WIL

Hoe gaat WIL om met persoonsgegevens?

Hier leggen we uit hoe we binnen WIL omgaan met persoonsgegevens. Het is de bedoeling dat iedereen die werkzaamheden voor en/of namens WIL uitvoert zich aan deze regels houdt.

1. Wat zijn persoonsgegevens?
Voordat we kunnen uitleggen hoe WIL omgaat met persoonsgegevens, is het van belang om eerst duidelijk uit te leggen wat persoonsgegevens precies zijn.

> ***Persoonsgegevens*** *zijn de gegevens over een persoon die ervoor zorgen dat een persoon* ***identificeerbaar is****, of* ***geïdentificeerd kan worden****. Een persoonsgegeven kan* ***direct of indirect*** *naar een persoon* ***herleiden****.*

Aan de hand van een naam of adres is zonder veel omwegen vast te stellen om welke persoon het gaat. Maar ook als er meerdere gegevens gecombineerd moeten worden om vast te stellen om wie het gaat, kan er sprake zijn van een persoonsgegeven. Zo kan een IP-adres, in combinatie met andere gegevens,

herleidbaar zijn naar een specifieke persoon. De gegevens die iets zeggen over een bepaald persoon in de database van WIL zijn ook voorbeelden van persoonsgegevens.

Via WIL kunnen diverse persoonsgegevens worden verwerkt. Hierbij gaat het bijvoorbeeld om:
- NAW-gegevens;
- Geboortedatums;
- Geslacht;
- E-mailadressen;
- Burgerservicenummers;
- Financiële gegevens (zoals inkomen);
- Gegevens over iemands gezondheid;
- Etc.

Met persoonsgegevens moet je zorgvuldig omgaan. Stel daarom telkens de vraag of je te maken hebt met persoonsgegevens bij jouw werkzaamheden. Om die vraag te beantwoorden is het van belang of iemand met een redelijke inspanning kan worden geïdentificeerd. Belangrijk om daarbij in gedachte te houden is dat het begrip 'persoonsgegeven' ruim is. Een gegeven is al snel een persoonsgegeven.

Ga je persoonsgegevens verwerken?	
Ja *De AVG en dit privacybeleid zijn van toepassing. Ga verder naar punt 2.*	***Nee*** *De AVG en dit privacybeleid zijn niet van toepassing. Je kunt je werkzaamheden voortzetten.*

2. Wat zijn bijzondere en gevoelige persoonsgegevens?
Persoonsgegevens kunnen daarnaast nog aangemerkt worden als 'bijzonder', waarvoor extra strenge regels gelden. Daarom moet extra voorzichtig worden omgegaan met het verzamelen en verwerken van bijzondere en gevoelige persoonsgegevens.

> ***Bijzondere persoonsgegevens*** *zijn gegevens die direct of indirect iets zeggen over iemands* ***godsdienst*** *of* ***levensovertuiging, ras, politieke overtuiging, gezondheid, seksuele leven****, alsmede persoonsgegevens betreffende het* ***lidmaatschap van een vakbond****.*

Aangezien WIL voor de uitvoering van haar taken bijzondere persoonsgegevens kan verwerken, is het van belang dat medewerkers van WIL zich hiervan bewust zijn. Denk bijvoorbeeld aan gegevens over de gezondheid van medewerkers en cliënten. Voor de verwerking van bijzondere persoonsgegevens moet een wettelijke uitzonderingsgrond bestaan.

Persoonsgegevens kunnen ook als 'gevoelig' worden beschouwd. Daarvan is sprake als persoonsgegevens een aanzienlijke impact hebben op het leven van personen, maar niet als bijzondere persoonsgegevens kunnen worden beschouwd. Voorbeelden van dergelijke gevoelige persoonsgegevens zijn informatie over financiën, inkomen en burgerservicenummers (BSN). Als medewerkers van WIL gevoelige persoonsgegevens verwerken, dan dienen zij hier extra zorgvuldig mee om te gaan, omdat de impact van het verwerken potentieel groter is dan bij persoonsgegevens die niet bijzonder of gevoelig zijn.

Wat te doen? Ga je (op een structurele basis als nieuwe activiteit) bijzondere persoonsgegevens verwerken als onderdeel van je werk voor WIL, neem dan contact op met de FG.

Ga je bijzondere of gevoelige persoonsgegevens verwerken?	
Ja Zie toelichting bij "Wat te doen?". Ga verder naar punt 3.	***Nee*** *Ga verder naar punt 3.*

3. Wie is een betrokkene?
Een betrokkene is de natuurlijke persoon over wie de persoonsgegevens gaan. WIL heeft te maken met verschillende betrokkenen. Hierbij gaat het bijvoorbeeld om:
- Cliënten;
- Medewerkers;
- Sollicitanten;
- Websitebezoekers;
- Medewerkers van leveranciers;
- Medewerkers van partners; en
- Andere personen.

Dit privacybeleid is opgesteld om de rechten van de betrokkenen zo goed mogelijk te waarborgen.

4. Wat betekent 'verwerking' van persoonsgegevens?
Verwerking van persoonsgegevens omvat alles dat je doet met persoonsgegevens. Dit begrip is in de AVG zeer ruim geformuleerd, alle handelingen die je met persoonsgegevens verricht vallen binnen het bereik ervan. Denk bijvoorbeeld aan:

- het opslaan van persoonsgegevens (zoals Word- en Pdf-bestanden, of informatie op het intranet (zoals het WILplein));
- het verwijderen van persoonsgegevens (zoals het weggooien/vernietigen van documenten of gebruikersaccounts);
- het doorsturen van persoonsgegevens (zoals in e-mails); en
- het kopiëren van persoonsgegevens.

5. Wanneer mag je persoonsgegevens verwerken?
Er moet een wettelijke grondslag zijn voordat je persoonsgegevens mag verwerken. Daarbij kun je kiezen uit zes mogelijkheden:

a) de betrokkene heeft **toestemming** gegeven (bijvoorbeeld voor het ontvangen van een nieuwsbrief of het verwerken van (bijzondere) persoonsgegevens door WIL);
b) de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** met de betrokkene (bijvoorbeeld om lonen uit te betalen aan medewerkers van WIL op grond van een arbeidsovereenkomst);
c) de verwerking is noodzakelijk om de **vitale belangen** van de betrokkene te beschermen (bijvoorbeeld wanneer een medewerker acuut ziek wordt op het werk – deze grondslag komt zelden voor);
d) de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting** (bijvoorbeeld het bewaren en doorgeven van fiscale gegevens aan de Belastingdienst);
e) de verwerking is noodzakelijk voor de vervulling van een taak van **algemeen belang** of een taak voor het **openbaar gezag** (bijvoorbeeld het verwerken van NAW- en financiële gegevens voor het doen van uitkeringen aan cliënten op grond de Participatiewet of het verlenen van schuldhulpverlening aan cliënten op grond van de Wet gemeentelijke schuldhulpverlening);
f) de verwerking is noodzakelijk voor de behartiging van de **gerechtvaardigde belangen** van WIL (bijvoorbeeld voor beveiligingsdoeleinden).

Toelichting grondslag a: toestemming
Hoewel *toestemming* de bekendste grondslag is, is het niet de meest gewenste grondslag om persoonsgegevens te verwerken. Aan de grondslag *toestemming* zijn namelijk strenge voorwaarden verbonden, waaronder de wijze waarop toestemming dient te worden uitgevraagd en het bewijs dat geleverd moet kunnen worden van de gegeven toestemming. Bovendien kan de persoon zijn toestemming ook weer intrekken, waardoor je de persoonsgegevens niet meer mag verwerken. Daarom dien je eerst na te gaan of gebruik kan worden gemaakt van één van de overige grondslagen. Wanneer de overige grondslagen geen uitkomst bieden, dient pas te worden gekozen voor *toestemming*.

Wanneer WIL toestemming vraagt, is er vaak sprake van een machtsongelijkheid tussen WIL en de betrokken cliënten. Dit maakt het moeilijk om te waarborgen dat de toestemming daadwerkelijk vrijelijk wordt gegeven. In dergelijke gevallen is toestemming geen werkbare grondslag voor de verwerking van persoonsgegevens.
In sommige situaties kan toestemming echter wel een werkbare grondslag zijn, bijvoorbeeld wanneer deze noodzakelijk is voor het bieden van integrale hulp en ondersteuning, zoals het delen van gegevens tussen verschillende teams binnen WIL. Gezien de kwetsbare positie van cliënten in ons sociaal domein is het belangrijk dat WIL in de meeste gevallen geen toestemming vraagt. In de situaties waarin toestemming wel gevraagd wordt, dient WIL zorgvuldig en verantwoordelijk om te gaan met de verkregen toestemming, zoals hieronder beschreven.

Om ervoor te zorgen dat op de juiste manier om toestemming wordt gevraagd, dient rekening gehouden te worden met het volgende:

- Toestemming dient **vrijwillig** te zijn
  De persoon die toestemming geeft mag niet gedwongen worden om toestemming te geven. De betrokkene moet toestemming kunnen weigeren, zonder dat daar nadelige gevolgen aan kunnen kleven. Een voorbeeld van een situatie waarin toestemming zelden vrijwillig kan worden gegeven is wanneer een werkgever toestemming vraagt aan een werknemer. Dit omdat er tussen beiden een gezagsrelatie aanwezig is.
- Toestemming dient **specifiek** te zijn
  De toestemmingsvraag dient in begrijpelijke/duidelijke taal te worden gesteld en mag niet zijn verstopt in een grote lap tekst (bijvoorbeeld algemene voorwaarden). De toestemmingsvraag moet gescheiden zijn van andere zaken.
- De persoon die toestemming geeft moet worden **geïnformeerd**

Er dient exact te worden aangegeven wat er precies met de persoonsgegevens gaat gebeuren én er dient te worden verwezen naar de privacyverklaring waarin meer informatie wordt gegeven.

- Toestemming dient **ondubbelzinnig** te zijn
  Er mag geen twijfel bestaan dat de persoon die toestemming geeft, ook écht heeft bedoeld om die toestemming te geven. Dit kan bijvoorbeeld gewaarborgd worden door een vakje actief aan te vinken.
- Toestemming dient te allen tijde te kunnen worden **ingetrokken**
  De persoon die toestemming geeft, mag deze altijd intrekken. Het intrekken van de toestemming dient net zo gemakkelijk te kunnen worden uitgevoerd als het geven van de toestemming. Hierover dient hij te worden geïnformeerd. De persoonsgegevens dienen dan zo snel mogelijk te worden verwijderd, tenzij deze nog nodig zijn en op basis van een andere grondslag verwerkt kunnen worden.

Het is belangrijk dat achteraf kan worden aangetoond dat toestemming is verkregen. Daarom dient de toestemmingsverklaring zorgvuldig te worden gelogd (indien mogelijk) en bewaard.
Ga altijd eerst na of er gebruik kan worden gemaakt van één van de overige grondslagen in plaats van toestemming.

Is op een juiste wijze om toestemming gevraagd voor de verwerking van persoonsgegevens?	
Ja *Je kunt gebruik maken van de grondslag toestemming. Ga verder naar punt 6.*	***Nee*** *Zoek een andere grondslag. Als er geen andere grondslag is neem je contact op met de FG.*

Toelichting grondslag b: uitvoering van een overeenkomst
Persoonsgegevens mogen worden verwerkt als dit nodig is om een overeenkomst uit te voeren. Dit betekent dat alleen van deze grondslag gebruik kan worden gemaakt als er afspraken zijn gemaakt en de persoonsgegevens noodzakelijk zijn om die afspraak na te komen. Dit is bijvoorbeeld het geval als gegevens van een medewerker in het personeelsdossier moeten worden vastgelegd om de arbeidsovereenkomst na te komen. Een ander voorbeeld is het geval waarin WIL met een commerciële partij een overeenkomst sluit en het voor een goede uitvoering van de overeenkomst noodzakelijk is om bepaalde persoonsgegevens te verwerken, bijvoorbeeld het e-mailadres van contactpersonen.

Let op! Gezondheidsgegevens kunnen niet worden verwerkt met de grondslag uitvoering van een overeenkomst. Dit zijn immers bijzondere persoonsgegevens waarvoor meer nodig is.

Is er een overeenkomst gesloten met de betrokkene en is het verwerken van persoonsgegevens nodig om de afspraken na te komen?	
Ja *Je kunt gebruik maken van de grondslag uitvoering van een overeenkomst. Ga verder naar punt 6.*	***Nee*** *Zoek een andere grondslag. Als er geen andere grondslag is neem je contact op met de FG.*

Toelichting grondslag d: het vervullen van een wettelijke verplichting
Persoonsgegevens mogen worden verwerkt als dit nodig is voor het vervullen van een eigen wettelijke verplichting. Het moet niet mogelijk zijn om de wettelijke verplichting te vervullen zonder dat de persoonsgegevens worden verwerkt. Denk bijvoorbeeld aan het verplicht delen van bepaalde persoonsgegevens met de Belastingdienst.

Is er een wettelijke verplichting waarvoor het nodig is dat er persoonsgegevens worden verwerkt?	
Ja *Je kunt gebruik maken van de grondslag wettelijke verplichting. Ga verder naar punt 6.*	***Nee*** *Zoek een andere grondslag. Als er geen andere grondslag is neem je contact op met de FG.*

Toelichting grondslag e: het vervullen van een taak van algemeen belang of een taak voor het openbaar gezag
Als de verwerking van persoonsgegevens noodzakelijk is om (meestal als overheid) een door de wet gegeven taak uit te oefenen, of om een wettelijke bevoegdheid uit te oefenen, dan is deze grondslag van toepassing. Het gaat daarbij om taken en bevoegdheden die door de wet aan een organisatie zijn gegeven. Voor WIL is dit de belangrijkste grondslag!
Het moet voor mensen duidelijk zijn dat WIL hun persoonsgegevens verwerkt om die specifieke wettelijke taak/taken uit te oefenen. Daarnaast moet de verwerking van de persoonsgegevens noodzakelijk zijn om de publieke taak – zoals het verstrekken van uitkeringen - goed te kunnen vervullen.

WIL dient hiervoor wettelijk aangewezen te zijn. Aangezien WIL een gemeenschappelijke regeling op basis van de Wet gemeenschappelijke regelingen is, verloopt de wettelijke aanwijzing van bevoegdheden getrapt. In de Participatiewet en de Wet gemeentelijke schuldhulpverlening zijn gemeenten wettelijk aangewezen als verantwoordelijke instanties. De gemeenten die deelnemen aan WIL hebben vervolgens hun bevoegdheden op basis van deze wetten gedelegeerd aan WIL, waardoor WIL bevoegd is om persoonsgegevens te verwerken voor de uitvoering van deze wettelijke taken.

Is er een taak van algemeen belang of een taak voor het openbaar gezag waarvoor het nodig is dat er persoonsgegevens worden verwerkt?	
Ja *Je kunt gebruik maken van de grondslag taak van algemeen belang of een taak voor het openbaar gezag. Ga verder naar punt 6.*	***Nee*** *Zoek een andere grondslag. Als er geen andere grondslag is neem je contact op met de FG.*

Toelichting grondslag f: gerechtvaardigd belang
De grondslag gerechtvaardigd belang is een belangrijke grondslag. Een beroep op deze grondslag kan uitkomst bieden in het geval dat WIL een bepaald belang heeft bij de verwerking van persoonsgegevens, maar geen beroep kan doen op de grondslag ‘taak van algemeen belang of taak van openbaar gezag’. Denk bijvoorbeeld aan beveiligingsbelangen.

Het is belangrijk op te merken dat de mogelijkheden voor WIL, als overheidsinstantie, om zich op deze grondslag te beroepen beperkt zijn. Dit komt omdat WIL haar publieke taken doorgaans uitvoert op basis van een wettelijke verplichting (grondslag e). Overheidsorganisaties mogen in principe geen beroep doen op "gerechtvaardigd belang" voor de verwerking van persoonsgegevens in het kader van de uitvoering van hun publieke taken. Alleen in uitzonderlijke gevallen, zoals bij de beveiliging van systemen of niet-publieke activiteiten, zou WIL een beroep kunnen doen op deze grondslag.

Om gebruik te kunnen maken van de grondslag gerechtvaardigd belang dient een driestappentoets te worden uitgevoerd:

1. **Is er een gerechtvaardigd belang bij het verwerken van persoonsgegevens?**
   Het verwerken van persoonsgegevens dient met andere woorden een toegevoegde waarde te hebben voor WIL of een derde. Erkende gerechtvaardigde belangen zijn bijvoorbeeld het tegengaan van fraude, oplichting of ander onrechtmatig gedrag. En ook het beschermen van de privésfeer of het nakomen van zorgplichten voor werknemers en/of cliënten.
2. **Is de verwerking van persoonsgegevens nodig met het oog op dit belang?**
   De verwerking van persoonsgegevens moet nodig zijn om het gerechtvaardigd belang te kunnen behartigen. Dit betekent dat na dient te worden gegaan of het überhaupt nodig is om de persoonsgegevens te verwerken, en of de persoonsgegevens die worden verwerkt wel allemaal noodzakelijk zijn met het oog op het (gerechtvaardigd) belang. Hierbij dient getoetst te worden aan de zogeheten eisen van proportionaliteit en subsidiariteit.
   Proportionaliteit betekent dat het verwerken van de persoonsgegevens in verhouding dient te staan tot het te bereiken doel. De eis van subsidiariteit houdt in dat het doel niet op een andere manier, die minder inbreuk maakt op de privacy van betrokkene(n), kan worden bereikt.
3. **Weegt het belang van de organisatie zwaarder dan het belang van de persoon van wie de persoonsgegevens zijn?**
   Hierbij dient specifiek een afweging te worden gemaakt tussen de privacybelangen van de betrokkene(n) en het gerechtvaardigd belang dat de organisatie heeft bij de verwerking van persoonsgegevens. Daarbij dienen er maatregelen te worden genomen die de privacy van de betrokkene(n) beschermen. Denk daarbij aan het vooraf informeren in lijn met de AVG en het op een passende manier beschermen van de persoonsgegevens en de mogelijkheid om bezwaar te maken.

Ga er niet te snel vanuit dat je de grondslag gerechtvaardigd belang kunt gebruiken. Dit is een belangenafweging waarbij het belang van WIL (of een derde) zwaarder moet wegen dan het recht op privacy van de betrokkene(n) (zoals een cliënt of een medewerker).
Bovendien mogen overheidsorganisaties geen gebruik maken van de grondslag gerechtvaardigd belang als het gaat om de uitoefening van hun wettelijke taak.

Met andere woorden: WIL kan de grondslag gerechtvaardigd belang niet gebruiken in haar relatie met cliënten, maar bijvoorbeeld wel als het gaat om de beveiliging van het gebouw en de personen die in het gebouw aanwezig zijn.

Neem altijd contact op met de FG als je bij het uitvoeren van nieuwe werkzaamheden van plan bent om gebruik te maken van de grondslag gerechtvaardigd belang voor het verwerken van persoonsgegevens.

Is er voldaan aan de driestappentoets?	
Ja *Zelfs dan kan je mogelijk geen gebruik maken van de grondslag gerechtvaardigd belang. Neem altijd eerst contact op met de FG. Ga verder naar punt 6.*	***Nee*** *Zoek een andere grondslag. Als er geen andere grondslag is neem je contact op met de FG.*

6. Voor welk doel mag je de persoonsgegevens verwerken?
Naast het hebben van een grondslag om persoonsgegevens te mogen verwerken (zie punt 5), moet je ook een doel hebben om de persoonsgegevens te verwerken. Je moet, met andere woorden, een goede reden hebben om iemands persoonsgegevens te verwerken. Persoonsgegevens mogen alleen voor de doeleinden worden verwerkt, waarvoor ze zijn verzameld. Als je bijvoorbeeld persoonsgegevens verwerkt om een cliënt te identificeren, mag je deze persoonsgegevens niet zomaar voor een ander doel gebruiken.

Is het toch nodig om persoonsgegevens voor een ander doeleinde te gebruiken dan waarvoor deze zijn verzameld, neem dan contact op met de PO of, indien de PO niet tijdig beschikbaar is, met de FG.

Heb je een doel (goede reden) voor het verwerken van persoonsgegevens? Kies bij twijfel altijd 'nee'.	
Ja *Je hebt een doel voor het verwerken van persoonsgegevens. Ga verder naar punt 7.*	***Nee*** *Zonder een doel (goede reden) mag je niets met persoonsgegevens doen. Neem bij twijfel contact op met de PO of FG.*

7. Welke persoonsgegevens mag ik verwerken?
Je mag alleen die persoonsgegevens verwerken die noodzakelijk zijn om je werk goed uit te kunnen voeren. Stel dus, voordat je persoonsgegevens gaat verwerken, vast of het verwerken van deze persoonsgegevens ook echt noodzakelijk is, of slechts wenselijk.

Twijfel je of het wel noodzakelijk is om de persoonsgegevens te verwerken? Neem dan contact op de PO.

Is het noodzakelijk om de persoonsgegevens te verwerken? Kies bij twijfel altijd 'nee'.	
Ja *Het verwerken van persoonsgegevens is noodzakelijk. Ga verder naar punt 8*	***Nee*** *Je mag alleen persoonsgegevens verwerken als dat noodzakelijk is. Neem contact op met de PO.*

8. Welke persoonsgegevens mag je bewaren en voor hoe lang?
Veel organisaties willen graag zo veel mogelijk gegevens zo lang mogelijk bewaren. Met het oog op privacy, is dat echter niet toegestaan. Houd je dan ook aan de volgende regels:
- Bewaar **niet meer** persoonsgegevens **dan nodig is**;
- Bewaar persoonsgegevens **niet langer dan nodig is**.

Bij iedere verwerkingsactiviteit moet je controleren of alle te gebruiken persoonsgegevens wel noodzakelijk zijn. Het is belangrijk om telkens kritisch te kijken naar de noodzakelijkheid voor het verzamelen én bewaren van persoonsgegevens.

Heb je de persoonsgegevens niet meer nodig? Dan dien je deze te verwijderen. In het verwerkingsregister zijn de bewaartermijnen opgenomen (zie punt 11). Daarin kun je zien dat sommige persoonsgegevens langer bewaard moeten blijven dan andere. Controleer periodiek je bestanden en e-mails op persoonsgegevens die niet langer nodig zijn.

Bewaar niet meer persoonsgegevens dan nodig is. En bewaar deze persoonsgegevens niet langer dan nodig is. Heb je persoonsgegevens niet meer nodig? Verwijder deze dan. Neem bij twijfel contact op met de PO of FG.

9. Wat is een verwerkingsverantwoordelijke en een verwerker?
Organisaties kunnen verwerkingsverantwoordelijke en verwerker zijn voor verschillende informatie.

*De **verwerkingsverantwoordelijke** is de partij die het doel en de middelen van de verwerking vaststelt. Wanneer een organisatie persoonsgegevens verwerkt namens een andere organisatie, is deze organisatie een **verwerker**.*

Wanneer een organisatie het *waarom* en het *hoe* van de gegevensverwerking vaststelt, dan is deze partij een verwerkingsverantwoordelijke. WIL is een verwerkingsverantwoordelijke voor de persoonsgegevens van cliënten, maar ook van persoonsgegevens van leveranciers, websitebezoekers en andere personen die contact met ons opnemen. Daarnaast is WIL verwerkingsverantwoordelijke voor de personeelsgegevens die in het personeelsdossier worden opgeslagen, omdat het *waarom* en het *hoe* in het kader van de verwerking van deze persoonsgegevens worden vastgesteld door WIL.

Indien WIL gegevensverwerkingen ten aanzien van persoonsgegevens verricht in opdracht van – ten behoeve en op instructie van – andere organisaties, dan is WIL een verwerker.

In het geval WIL verwerkingsverantwoordelijke is, rust de verplichting ten aanzien van het sluiten van een verwerkersovereenkomst op WIL. In het geval WIL verwerker is, rust deze verplichting op de verwerkingsverantwoordelijke. Desondanks is het in het laatste geval ook wenselijk voor WIL om een verwerkersovereenkomst te sluiten en kan ook WIL hierin het initiatief nemen.

10. Wat is een verwerkersovereenkomst en een data- uitwisselingsovereenkomst?
Een verwerkersovereenkomst is nodig indien WIL besluit om een verwerking deels of geheel uit te besteden aan een externe organisatie die in opdracht van WIL persoonsgegevens gaat verwerken. Denk bijvoorbeeld aan gemeente Houten, die onder andere de opslag verzorgt van de door WIL verwerkte persoonsgegevens; of aan AFAS, die het HR-systeem levert waarin personeelsgegevens van medewerkers van WIL worden verwerkt. WIL geeft in het laatstgenoemde geval opdracht om de personeelsgegevens te verwerken. Verwerkers zijn vaak (maar niet altijd) leveranciers van software of hostingproviders.

In een verwerkersovereenkomst spreek je onder andere af wat een verwerker mag doen met de persoonsgegevens, welke beveiligingsmaatregelen een verwerker dient te treffen en welke stappen genomen moeten worden als persoonsgegevens gelekt zijn door een datalek (zie punt 14).

Wanneer WIL structureel persoonsgegevens verstrekt aan een externe organisatie, die geen persoonsgegevens verwerkt in opdracht van WIL, maar voor eigen of gezamenlijke doeleinden, dan hoeft er geen verwerkersovereenkomst gesloten te worden tussen partijen. Er is dan immers geen sprake van een “verwerkingsverantwoordelijke-verwerker”-relatie. Van een dergelijke situatie is sprake bij verwerking van persoonsgegevens door bijvoorbeeld een arbodienst of de Belastingdienst.

Als er sprake is van het verstrekken van persoonsgegevens aan een externe organisatie die voor eigen doeleinden persoonsgegevens verwerkt (en dus zelfstandig verwerkingsverantwoordelijke is), dan is een data-uitwisselovereenkomst raadzaam, maar niet verplicht.

Een data-uitwisselovereenkomst is wel verplicht als er sprake is van het verstrekken van persoonsgegevens aan een externe organisatie die voor gezamenlijke doeleinden persoonsgegevens verwerkt (er zijn dan dus twee gezamenlijke verwerkingsverantwoordelijken). In een data-uitwisselovereenkomst leg je onder andere vast waar welke partij voor verantwoordelijk is. In vergelijking met een verwerkersovereenkomst ligt de rolverdeling in een data-uitwisselovereenkomst anders.

Als er sprake is van het verstrekken van persoonsgegevens aan een externe organisatie die is gevestigd in de Verenigde Staten, dan hangen de voorwaarden af van de deelname van de externe organisatie aan het Data Privacy Framework. Dit framework bestaat uit afspraken voor veilige gegevensoverdracht naar de Verenigde Staten. Voordat gegevensoverdracht plaatsvindt, moet men controleren of de organisatie in de VS aan het Data Privacy Framework deelneemt. De deelnemende organisaties zijn te vinden via deze website. Als de externe organisatie aan het Data Privacy Framework deelneemt, dan mogen persoonsgegevens van WIL worden doorgegeven zonder extra maatregelen. Als de organisatie echter niet deelneemt, dan zijn er specifieke voorwaarden van toepassing; bijvoorbeeld het gebruik van bepaalde doorgifte-instrumenten en het nemen van extra maatregelen, zoals in de volgende alinea staat beschreven.

Als er sprake is van het verstrekken van persoonsgegevens aan een externe organisatie die is gevestigd buiten de Europese Economische Ruimte (‘EER’) en niet deelneemt aan de Data Privacy Framework, dan dienen er aanvullende maatregelen genomen te worden. Concreet betekent dit dat WIL moet borgen dat persoonsgegevens worden doorgegeven naar een zogenaamd adequaat land of dat er passende waarborgen worden getroffen zoals het sluiten van zogenaamde ‘Standard Contractual Clauses’.

Ga je structureel persoonsgegevens verstrekken aan (of ontvangen van) een externe organisatie bij het uitvoeren van nieuwe activiteiten? Neem contact op met een adviseur van het team Juridische

Zaken (hierna: "JZ"). JZ volgt dan de 'Handleiding voor het maken van afspraken met externe organisaties bij het verwerken van persoonsgegevens' in Bijlage 1 en kan de overeenkomst opstellen. De PO en FG kunnen gecontacteerd worden door JZ om te adviseren over de verwerkersovereenkomsten en data-uitwisselovereenkomsten.

Let op! JZ regelt dit onderdeel. Dit hoef je dus als medewerker van WIL (bij een ander team dan JZ) niet zelf te doen. Voor jou als medewerker is het van belang dat je contact opneemt met een adviseur van het team Juridische Zaken als je structureel persoonsgegevens gaat verstrekken aan (of ontvangen van) een nieuwe externe organisatie.

Ga je structureel gegevens verstrekken aan (of ontvangen) van externe organisaties? Kies bij twijfel altijd 'ja'.	
Ja Als de externe organisaties geen verwerker zijn moet WIL een grondslag hebben voor het verstrekken van persoonsgegevens. WIL moet daarnaast met externe organisaties afspraken maken, die worden vastgelegd in een verwerkersovereenkomst of data-uitwisselovereenkomst. Neem contact op met JZ. JZ volgt dan de '***Handleiding voor het maken van afspraken met externe organisaties bij het verwerken van persoonsgegevens'*** in Bijlage 1.	***Nee*** *Ga verder naar punt 11.*

11. Wat is een verwerkingsregister?
Het is wettelijk verplicht om een verwerkingsregister te hebben en actueel te houden. Het register is een overzicht van de gegevensverwerkingen die plaatsvinden binnen WIL. Hierin staan onder andere de soorten betrokkenen, soorten persoonsgegevens, grondslagen, doelen en bewaartermijnen. Denk bijvoorbeeld aan de sollicitatieprocedure, waarbij diverse persoonsgegevens van een sollicitant worden verwerkt ter voorbereiding op een eventueel te sluiten arbeidsovereenkomst. Of aan persoonsgegevens van de aanvragers van een bijstandsuitkering of schuldhulpverlening.
Het register wordt beheerd door de FG. Als je, als een gevolg van nieuwe of gewijzigde werkzaamheden, persoonsgegevens gaat verwerken, dan dient dat in het verwerkingsregister vermeld te worden. Neem hiervoor contact op met de FG.

Als je persoonsgegevens gaat verwerken dan moet dat in het verwerkingsregister vermeld worden. Neem hiervoor contact op met de FG.

12. Beveiligingsmaatregelen
Als je met persoonsgegevens in aanraking komt, dan is het belangrijk daar zorgvuldig mee om te gaan. De AVG schrijft voor dat elke organisatie passende beveiligingsmaatregelen moet treffen. WIL heeft de nota 'Strategisch Informatiebeveiligingsbeleid 2023-2026' opgesteld waarin is opgenomen hoe WIL informatie beveiligt.

13. Versturen van persoonsgegevens via e-mail?
E-mailberichten bevatten vaak persoonsgegevens. Wanneer je bestanden verstuurt per mail, dan is het belangrijk om rekening te houden met de volgende punten:

- Verstuur alle berichten, waarin persoonsgegevens zijn opgenomen, uitsluitend via ZIVVER;
- Verstuur nooit meer persoonsgegevens dan strikt noodzakelijk is;
- Controleer vóór het verzenden alle personen en organisaties aan wie het bericht met persoonsgegevens zal worden verstuurd en verwijder alle personen en organisaties voor wie het niet noodzakelijk is om toegang tot de persoonsgegevens verkrijgen.
- Mocht je per ongeluk berichten met persoonsgegevens via ZIVVER naar een onjuiste afzender hebben gestuurd, dan dienen nog niet geopende berichten direct te worden ingetrokken.

14. Wat is een datalek en wat moet ik doen bij een datalek ?
Ondanks alle beveiligingsmaatregelen kan het voorkomen dat er iets gebeurt met persoonsgegevens wat niet de bedoeling was. Dat kan resulteren in een datalek. Een datalek is:

> *Een inbreuk op de beveiliging die **per ongeluk of op onrechtmatige wijze** leidt tot de **vernietiging**, het **verlies**, de **wijziging** of de ongeoorloofde **verstrekking** van of de ongeoorloofde **toegang** tot doorgezonden, opgeslagen of anderszins verwerkte **gegevens**.*

In het kort: alles wat 'verkeerd gaat' met persoonsgegevens. Een datalek ligt altijd op de loer wanneer persoonsgegevens worden verwerkt. Fouten maken is immers menselijk. Een datalek kan dan ook iedereen overkomen. Het belangrijkste is om een datalek op de juiste manier af te handelen, als het zich voordoet.

Er geldt een interne meldplicht als er sprake is van een datalek. Er is bijvoorbeeld sprake van een datalek als er persoonsgegevens inzichtelijk zijn geworden voor mensen (zowel intern als extern) waarvoor de persoonsgegevens niet toegankelijk horen te zijn of wanneer de persoonsgegevens verloren zijn gegaan, terwijl dat niet de bedoeling was. Ook wanneer persoonsgegevens anderszins onrechtmatig worden verwerkt óf wanneer dit niet valt uit te sluiten, is er sprake van een datalek. Hierna volgt een lijst van concrete voorbeelden van datalekken:

- Het versturen van een e-mailbericht waarbij de ontvangers in de 'CC' staan, terwijl zij elkaars e-mailadres niet behoren te kennen (deze moeten dus in de 'BCC');
- Persoonsgegevens verspreiden buiten de organisatie, terwijl je ze intern wilde delen;
- Het (mail)account van een gebruiker is gehackt, waardoor informatie gestolen kan worden door een cybercrimineel;
- Laptop of werktelefoon kwijtgeraakt of gestolen;
- Een beschikking van de ene cliënt is per ongeluk bij die van een andere cliënt gevoegd, waardoor laatstgenoemde cliënt toegang heeft gekregen tot de persoonsgegevens van eerstgenoemde.

Denk je dat er (mogelijk) sprake is van een datalek? **Meld dit dan direct bij de PO**. Het is belangrijk dat dit direct gebeurt, omdat sommige datalekken **binnen 72 uur** na ontdekking gemeld dienen te worden aan de Autoriteit Persoonsgegevens ('**AP**'). De PO zal dan waar nodig mitigerende maatregelen (laten) treffen om het datalek te stoppen, in de toekomst te voorkomen en/of de gevolgen van het datalek zoveel als mogelijk te beperken. Deze maatregelen zijn in de regel effectiever, als zij in een vroeg stadium worden genomen.
Zie de onderstaande procedure.

De onderstaande beslisboom kan gebruikt worden om te bepalen of er sprake is van een datalek, en zo ja, of melding moet worden gedaan aan de AP en aan de betrokkene(n):

Voor het melden van datalekken hanteren wij de volgende procedure:

1. Een datalek begint altijd met een inbreuk op de beveiliging: een inbreuk op de integriteit, vertrouwelijkheid of beschikbaarheid van gegevens. Dit noemen we een **beveiligingsincident**. Zijn daar ook persoonsgegevens bij betrokken, dan kan er sprake zijn van een datalek.
2. **Melden beveiligingsincident aan de PO**
   Als er binnen WIL een beveiligingsincident plaatsvindt, dient de ontdekker van het beveiligingsincident dit te melden aan de PO. De PO is bereikbaar via de volgende contactgegevens:
   - E-mail: privacy@wil-lekstroom.nl.

   De PO handelt het datalek samen met jou af.
3. **Inventariseren**
   De ontdekker van het beveiligingsincident vermeldt bij de melding van een (potentieel) datalek de volgende informatie:
   - Wie heeft het beveiligingsincident gemeld (ontdekker)?
   - Wat is er gebeurd?
   - Wanneer heeft het beveiligingsincident plaatsgevonden en wanneer is het ontdekt?
   - Hoe heeft het beveiligingsincident plaatsgevonden?
   - Om welke gegevens van welke personen gaat het?

- Om hoeveel gegevens van hoeveel personen gaat het?
- Welke systemen zijn betrokken bij/geraakt door het beveiligingsincident?
- Wat is er al gedaan om het beveiligingsincident op te lossen/in de toekomst te voorkomen/de gevolgen van het beveiligingsincident te beperken?

Indien dit niet voldoende is om het incident te beoordelen en af te handelen, zal de PO contact met de ontdekker opnemen voor meer informatie. Zorg er daarom voor dat je als ontdekker van het (potentiële) datalek beschikbaar bent om eventuele vragen te beantwoorden.

4. **Is het beveiligingsincident een datalek?**
Een beveiligingsincident is nog geen datalek. Een beveiligingsincident wordt pas een datalek wanneer de inbreuk gevolgen heeft voor de persoonsgegevens die WIL verwerkt. Die gevolgen kunnen bijvoorbeeld bestaan uit het verlies van persoonsgegevens, of een onrechtmatige verwerking daarvan. Wanneer de PO voldoende informatie heeft verzameld, beoordeelt hij op basis van de antwoorden op de vragen bij de vorige stap in de procedure of er sprake is van een datalek. De PO kan de FG hieromtrent om advies vragen.
5. **Dient het datalek gemeld te worden aan de AP?**
Niet alle datalekken hoeven gemeld te worden aan de AP. Een datalek moet enkel gemeld worden aan de AP indien er sprake is van een risico voor de rechten en vrijheden van de betrokkene(n). Dit risico is aanwezig in twee situaties:
   - Bij een *kwantitatief* ernstig lek (hiervoor kijk je naar de hoeveelheid betrokken persoonsgegevens);
   - Bij een *kwalitatief* ernstig lek (hiervoor kijk je naar de gevoeligheid van de betrokken persoonsgegevens).

   Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek' dient er daarom rekening gehouden te worden met de hoeveelheid persoonsgegevens en met het type persoonsgegevens. Telkens dient een afweging te worden gemaakt of een datalek gemeld moet worden aan de AP. Hierbij zijn ook nog andere factoren van belang. Om deze afweging te kunnen maken beantwoordt de PO de volgende vragen:
   - Wat is er precies gebeurd (is er sprake van een intern/extern datalek)?
   - Welke gegevens van welke personen zijn betrokken bij het datalek?
   - Om hoeveel gegevens en personen gaat het?
   - Waarom is het wel/geen datalek dat gemeld moet worden?
   - Wat zijn de (mogelijke) gevolgen van het datalek?
   - Wie zijn er reeds geïnformeerd?
   - Wat zijn de te nemen vervolgstappen (melding aan de AP/betrokkene(n))?

   Op basis van de antwoorden op deze vragen, bepaalt de PO of er sprake is van een datalek dat gemeld dient te worden of niet. Van een datalek dat gemeld dient te worden, is bijvoorbeeld sprake wanneer er veel gegevens van één medewerker of cliënt van WIL gelekt zijn of gegevens van heel veel medewerkers of cliënten van WIL. Maar van een datalek dat gemeld dient te worden is ook sprake wanneer de gelekte persoonsgegevens gevoelig zijn. Te denken valt dan bijvoorbeeld aan persoonsgegevens over de gezondheid, over de financiële of economische situatie van de betrokkene, of als de persoonsgegevens kunnen leiden tot stigmatisering van de betrokkene. De PO kan voor advies terecht bij de FG.
6. **Melden aan de AP**
Brengt het datalek een risico voor de rechten en vrijheden van de betrokkene(n) met zich mee, dan moet er dus een melding worden gedaan bij de AP. De PO of de FG zal het datalek melden. Voor een datalek geldt als termijn dat het datalek zo snel mogelijk, maar uiterlijk binnen 72 uur na ontdekking, aan de AP gemeld moet worden via deze website. Overschrijding van de hierboven genoemde termijn is geen reden voor het niet melden bij de AP, maar de PO of de FG zal dan bij de melding aan moeten geven dat de termijn niet is gehaald. Indien er waarschijnlijk sprake is van een datalek, maar cruciale informatie hierover nog ontbreekt, dan zullen de PO of de FG een voorlopige melding maken aan de AP. Zodra er voldoende informatie is verzameld over het incident, trekt de PO of de FG de melding in of vult de PO of de FG de voorlopige melding aan, afhankelijk van de inhoud van deze informatie.
7. **Dient het datalek gemeld te worden aan de betrokkene(n)?**
Het is mogelijk dat een datalek niet alleen aan de toezichthouder gemeld moet worden, maar ook aan de betrokkene(n). Dit is het geval wanneer het datalek een hoog risico inhoudt voor betrokkene(n). Er is sprake van een datalek met een **hoog risico**, wanneer het privéleven van de betrokkene(n) waarschijnlijk door het datalek wordt geschaad of kan worden geschaad. Voorbeelden daarvan zijn: identiteitsdiefstal of -fraude, financiële verliezen en reputatieschade. Als het gaat om persoonsgegevens van gevoelige aard, zoals gezondheids- of financiële gegevens, of om een grote hoeveelheid persoonsgegevens, dan dient er altijd een melding aan de betrokkene(n) gedaan

te worden, tenzij de persoonsgegevens beveiligd zijn (bijvoorbeeld beveiligd via tweefactor-authenticatie).

8. **Melden aan de betrokkene(n)**
De melding aan de betrokkene(n) wordt gedaan door JZ en dient zorgvuldig uitgevoerd te worden. De melding dient de volgende informatie te bevatten:

Melding datalek aan betrokkene(n)	
Omschrijving	Op [datum] heeft er bij WIL een datalek plaatsgevonden waarbij uw gegevens betrokken zijn. Het gaat daarbij om de volgende persoonsgegevens: [uitgebreide omschrijving].
Vragen?	Voor vragen kunt u contact opnemen met de FG van WIL, via [e-mail] of [telefoonnummer].
Wat kunt u doen?	Om de (mogelijke) gevolgen van dit datalek te beperken raden wij u aan om de volgende maatregelen te treffen: - [maatregelen]

Uiteraard is het verstandig om in een begeleidend schrijven de betrokkene(n) excuses aan te bieden en duidelijk te maken dat WIL het datalek inmiddels heeft gedicht (indien dat het geval is) en er alles aan zal doen om dergelijke gevallen in de toekomst te voorkomen.

9. **Datalek registreren in het datalekregister**
Heeft de PO geconstateerd dat er sprake is van een datalek, dan dient alle informatie die in de voorafgaande stappen is ingewonnen, intern geregistreerd te worden in het datalekregister. De PO zorgt voor het registreren van het datalek in het register.
Let op: ieder datalek dient geregistreerd te worden in het datalekregister, **ook datalekken die niet gemeld zijn** aan de AP en/of betrokkene(n).

15. Welke rechten hebben betrokkenen?
In de AVG is een aantal rechten opgenomen die betrokkenen hebben, namelijk:
- Recht op **inzage** en een kopie van de persoonsgegevens die WIL verwerkt;
- Recht op **rectificatie** (bijvoorbeeld wanneer het e-mailadres niet correct is);
- Recht op **verwijdering** (betrokkene wil dat zijn WIL-account wordt verwijderd);
- Recht op **beperking** (persoonsgegevens niet meer verwerken totdat een bezwaar of probleem is opgelost);
- Recht op **overdraagbaarheid** van persoonsgegevens;
- Recht van **bezwaar** (geldt bijvoorbeeld voor de privacyvriendelijke analytische cookies op de website); en
- Recht om **toestemming in te trekken** (voor het verwerken van persoonsgegevens).

In de privacy- en cookieverklaring die op de website van WIL staat, zijn de rechten van betrokkenen eveneens genoemd. Denk je dat (mogelijk) sprake is van een verzoek van een betrokkene om zijn rechten uit te oefenen? Meld dit dan direct bij JZ via privacy@WIL-lekstroom.nl en volg de stappen zoals beschreven in punt 16.

Denk je dat sprake is van een verzoek van een betrokkene om zijn of haar rechten uit te oefenen? Meld dit dan direct bij JZ en volg de stappen zoals beschreven in punt 16.

16. Wat moet je doen als een betrokkene een van zijn rechten uitoefent?
Het kan voorkomen dat een betrokkene vraagt om inzage van zijn persoonsgegevens, of dat een betrokkene vraagt om verwijdering van zijn dossier. Ontvang je een dergelijk verzoek van een betrokkene, neem dan direct contact op met de adviseurs van JZ via privacy@WIL-lekstroom.nl. Zij handelen het verzoek vervolgens (samen met jou) af door onderstaande stappen te nemen.

1. ***Zorg dat het verzoek van de betrokkene duidelijk is en licht de betrokkene in over het verloop van de afhandeling van zijn verzoek.***
Vraag altijd van welk recht de betrokkene gebruik wil maken als het verzoek niet duidelijk is. Ook is het belangrijk om uit te leggen binnen welke termijn je het verzoek afhandelt (zie stap 2).

   Bij een inzage-, verwijderings- of aanpassingsverzoek, kan de betrokkene, zoals een medewerker, dit tegenwoordig vaak al zelf regelen (bijvoorbeeld in zijn AFAS-account). Het is wel van belang te onderkennen dat ook persoonsgegevens die buiten de macht van betrokkene worden verwerkt, onder deze rechten vallen.
2. ***Vraag altijd om een bewijs van identificatie van de betrokkene die het verzoek doet.***

Zorg dat je kunt controleren of diegene die het verzoek doet, ook daadwerkelijk de persoon is bij wie de persoonsgegevens horen. Als een betrokkene namelijk niet is wie hij zegt te zijn loop je de kans dat je de gegevens van iemand anders verstrekt (bij een inzageverzoek). In dat geval heb je een datalek (zie punt 14).

Het identificeren van de betrokkene is op verschillende manieren mogelijk. Bijvoorbeeld door middel van:
- een reeds bij WIL bekend e-mailadres;
- een reeds bij WIL bekend telefoonnummer;
- het verwijzen naar (recente) concrete feiten en omstandigheden (bijvoorbeeld een specifiek telefoongesprek of een specifieke mailwisseling, met een medewerker van WIL), die vanzelfsprekend wel geverifieerd moeten worden;
- herkenning van de betrokkene, op het moment dat hij het verzoek doet (bijvoorbeeld a.d.h.v. diens uiterlijk en/of stem); of
- een meegestuurd (afgeschermd) kopie van een identiteitsdocument.

In geval van twijfel over de identiteit van de verzoeker (bijvoorbeeld naar aanleiding van het niet goed beantwoorden van voor de hand liggende vragen, het geven van ontwijkende antwoorden, het geven van tegenstrijdige informatie, etc.) is het van belang om met een hogere mate van zekerheid de identiteit van de betrokkene vast te stellen. In het uiterste geval kan van de betrokkene verlangd worden dat hij zich in persoon op het kantoor van WIL laat identificeren a.d.h.v. een geldig identiteitsdocument.
Daarnaast kan het, gelet op de omvang en/of de gevoeligheid van de persoonsgegevens, raadzaam zijn om de identiteit van de betrokkene met een hogere mate van zekerheid vast te stellen.

Het digitaal (of via de post) opvragen van een onafgeschermd (kopie) identiteitsdocument is in beginsel niet toegestaan, omdat een dergelijke verificatiewijze verder gaat dan noodzakelijk is.

3. ***Verzoek binnen één maand afhandelen (wettelijk verplicht).***
Kost het veel tijd om een verzoek af te handelen (wegens de complexiteit of de omvang), dan mag de termijn van een maand verlengd worden met maximaal 2 maanden. Je moet de betrokkene hier wel over informeren binnen de eerste maand. Let op! Hier dient zeer terughoudend mee te worden omgegaan. De termijn mag niet worden verlengd, omdat WIL bijvoorbeeld te weinig medewerkers in dienst heeft die het verzoek kunnen afhandelen of omdat de systemen niet goed zijn ingericht.

4. ***Verstrek niet meer persoonsgegevens dan noodzakelijk is, en doe dit alleen wanneer het de persoonsgegevens van de betrokkene zijn.***
In het geval je persoonsgegevens aan de betrokkene dient te verstrekken, zorg er dan voor dat dit alleen de persoonsgegevens zijn die de betrokkene wenst te ontvangen. Zorg er daarnaast voor dat hier geen persoonsgegevens van andere betrokkenen tussen zitten. De (privacy)rechten van andere betrokkenen dienen immers ook gewaarborgd te worden. Daarom worden hun persoonsgegevens in beginsel onleesbaar gemaakt. (NB: Wel bestaat er de mogelijkheid om aan andere betrokkenen toestemming te vragen om hun persoonsgegeven (al dan niet gedeeltelijk) leesbaar te houden.)

Indien de betrokkene niet duidelijk heeft aangegeven welke persoonsgegevens hij wenst te ontvangen, dan kan hem gevraagd worden om dit te specificeren.

Tip: bij een omvangrijk verzoek, verdient het in de regel aanbeveling om standaard om een specificatie te vragen.

De documenten met persoonsgegevens worden in beginsel beveiligd via ZIVVER verstrekt (met gebruikmaking van SMS-authenticatie).

5. ***Verzoek kosteloos afhandelen.***
In de AVG staat dat organisaties geen geld mogen vragen aan de betrokkene voor het afhandelen van een verzoek. Behalve wanneer het verzoek buitensporig is (lees: er gevraagd wordt om verschillende fysieke kopieën etc.).

Bijlage 1 – AVG: handleiding voor het maken van afspraken met externe organisaties bij het verwerken van persoonsgegevens

WIL verstrekt persoonsgegevens aan externe organisaties. Bijvoorbeeld aan de in WIL deelnemende gemeenten, maar dit kunnen ook andere partijen zijn. Hierbij moet WIL zich aan de regels van de AVG houden. De volgende informatie geeft je als medewerker van WIL een beeld van wat de adviseurs van JZ moeten doen als er structureel persoonsgegevens worden uitgewisseld met externe organisaties.

Let op! De adviseurs van JZ of de PO regelen dit. Dit hoef je dus als medewerker van WIL niet zelf te doen. Voor jou als medewerker van WIL is het van belang dat je contact opneemt met de adviseurs van JZ, de PO of de FG als je structureel persoonsgegevens gaat verstrekken aan (of ontvangen van) een nieuwe externe organisatie.

Afhankelijk van de situatie (zie hieronder, 5 verschillende situaties), moet WIL een zogeheten **grondslag** (punt 5) hebben om persoonsgegevens aan externe organisaties te verstrekken. Relevante grondslagen voor het verstrekken van persoonsgegevens zijn:

a) WIL heeft een ***wettelijke verplichting*** om persoonsgegevens te verstrekken;
b) de verwerking is noodzakelijk voor de vervulling van een taak van ***algemeen belang*** of een taak voor het ***openbaar gezag***;
c) WIL heeft ***toestemming*** aan de betrokkene gevraagd voor het verstrekken van persoonsgegevens.

WIL dient altijd eerst te bekijken of er een wettelijke plicht is of dat de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of een taak voor het openbaar gezag. Bij afwezigheid van deze grondslagen dient WIL af te wegen of er een gerechtvaardigd belang aanwezig is voor het verstrekken van persoonsgegevens. Als er geen gerechtvaardigd belang is, zal WIL toestemming moeten vragen aan de betrokkene voordat persoonsgegevens aan externe organisaties mogen worden verstrekt.

Naast het hebben van een grondslag moeten er ook **afspraken** (punt 10) worden gemaakt over het gebruik van persoonsgegevens.

Of er een grondslag aanwezig moet zijn, en zo ja, welke grondslag kan worden gebruikt en welke afspraken er gemaakt moeten worden is afhankelijk van de situatie. Hieronder worden vijf verschillende situaties beschreven:

Situatie 1: een opdrachtgever schakelt WIL in om persoonsgegevens in opdracht van de opdrachtgever te verwerken.
WIL zou in deze situatie voor haar werkzaamheden ingeschakeld worden door opdrachtgevers om (een deel van) de verwerking van persoonsgegevens uit te voeren. In deze situaties is de opdrachtgever een verwerkingsverantwoordelijke en WIL een verwerker.

WIL heeft in deze situatie **geen grondslag** nodig voor het verwerken van persoonsgegevens vanuit de opdrachtgever, aangezien de opdrachtgever hiervoor als verwerkingsverantwoordelijke moet zorgen. Wel dient er een verwerkersovereenkomst gesloten te worden.

De opdrachtgever bepaalt in deze situatie zelf *waarom* en *hoe* persoonsgegevens worden verwerkt. De opdrachtgever geeft instructies aan WIL, onder meer over de doelen waarvoor de persoonsgegevens gebruikt mogen worden.

Let op! Indien WIL, in afwijking van of buiten de opdracht persoonsgegevens verwerkt, dan kan WIL voor die verwerkingen gezien worden als verwerkingsverantwoordelijke.

Situatie 2: WIL schakelt als verwerker een externe organisatie in om persoonsgegevens in opdracht van WIL te verwerken.
Deze situatie sluit aan op situatie 1. WIL kan in deze situatie bij de werkzaamheden die zij uitvoert, in opdracht van haar opdrachtgevers, verschillende partijen inschakelen om (een deel van) de verwerking van persoonsgegevens aan uit te besteden. In deze situaties is WIL een verwerker en de externe organisatie een subverwerker.

WIL heeft in deze situatie **geen grondslag** nodig voor het verstrekken van persoonsgegevens aan deze subverwerkers. Wel dient er een **subverwerkersovereenkomst** gesloten te worden tussen WIL en de externe organisatie.

Situatie 3: WIL schakelt als verwerkingsverantwoordelijke een externe organisatie in om persoonsgegevens in opdracht van WIL te verwerken.

WIL schakelt bij haar werkzaamheden als verwerkingsverantwoordelijke verschillende partijen in om (een deel van) de verwerking van persoonsgegevens uit te voeren. In deze situaties is WIL een verwerkingsverantwoordelijke en de externe organisatie een verwerker. Denk bijvoorbeeld aan CompetenSYS (voor de verwerking van persoonsgegevens van cliënten door WIL in het kader van diagnostiek en matching). WIL is de verwerkingsverantwoordelijke voor de persoonsgegevens die van cliënten via de software van CompetenSYS verwerkt worden en CompetenSYS is de verwerker.

WIL heeft in deze situatie **geen grondslag** nodig voor het verstrekken van persoonsgegevens aan externe organisaties. Wel dient er een **verwerkersovereenkomst** gesloten te worden.

WIL bepaalt in deze situatie zelf *waarom* en *hoe* persoonsgegevens worden verwerkt. WIL geeft instructies aan de organisaties die worden ingeschakeld, onder meer over de te nemen beveiligingsmaatregelen en de doelen waarvoor de persoonsgegevens gebruikt mogen worden.

Situatie 4: WIL verstrekt persoonsgegevens aan externe organisaties, zodat externe organisaties deze kunnen inzetten voor eigen doeleinden. Het kan ook zo zijn dat WIL persoonsgegevens ontvangt van externe organisaties, zodat WIL deze kan inzetten voor eigen doeleinden.
WIL en de externe organisatie zijn in deze situatie zelfstandig verwerkingsverantwoordelijke. In deze situatie heeft WIL een **grondslag** nodig voor het verstrekken van persoonsgegevens aan externe organisaties.

Het is raadzaam – maar niet verplicht – om een **data-uitwisselovereenkomst** te sluiten met daarin afspraken over onder andere de wijze waarop de uitwisseling van persoonsgegevens plaats zal vinden en waar welke partij voor verantwoordelijk is.

WIL en de externe organisatie zijn in deze situatie zelfstandig verantwoordelijk voor het verwerken van dezelfde persoonsgegevens, omdat ze hier allebei eigen doeleinden voor hebben. Beide partijen bepalen zelf wat ze met deze persoonsgegevens gaan doen, *waarom* dit gebeurt en *hoe* de verwerking plaats zal vinden. Denk aan de situatie dat WIL persoonsgegevens van medewerkers uitwisselt met een arbodienst.

Situatie 5: WIL verstrekt persoonsgegevens aan externe organisaties om deze in te zetten voor doeleinden die gezamenlijk met de externe organisaties worden bepaald. Het kan ook zo zijn dat WIL persoonsgegevens ontvangt van externe organisaties, zodat WIL deze kan inzetten voor doeleinden die gezamenlijk met de externe organisaties worden bepaald.
WIL en de externe organisatie zijn gezamenlijk verantwoordelijk voor het verwerken van dezelfde persoonsgegevens, omdat ze hier allebei dezelfde doeleinden voor hebben.

In deze situatie heeft WIL een **grondslag** nodig voor het verstrekken van persoonsgegevens aan externe organisaties. Daarnaast dient WIL in een **data-uitwisselovereenkomst** afspraken te maken over onder andere de wijze waarop de uitwisseling van persoonsgegevens plaats zal vinden en waar welke partij voor verantwoordelijke is.

WIL en de externe organisatie zijn gezamenlijk verantwoordelijk voor het verwerken van dezelfde persoonsgegevens. Beide partijen bepalen samen wat ze met deze persoonsgegevens gaan doen, *waarom* dit gebeurt en *hoe* de verwerking plaats zal vinden.

Bijlage 2 – AVG: stappenplan voor het verstrekken (of ontvangen) van persoonsgegevens aan (of van) externe organisaties