



**Privacybeleid
Werkstichting Lage
Weide
=
ILW Parkmanagement
Lage Weide (PMLW)**

Inhoudsopgave

1.	Inleiding.....	3
2.	Definities	3
3.	Doel en reikwijdte	4
4.	Wet- en regelgeving	5
5.	Uitgangspunten	5
6.	Organisatie van privacy binnen PMLW	6
6.1	Richtinggevend	6
6.2	Sturend	6
6.3	Uitvoerend.....	6
7.	Verplichtingen en waarborgen	7
7.1	Register verwerkingen.....	7
7.2	Protocol privacy-incidenten en datalekken.....	7
7.3	Rechten van betrokkenen.....	8
7.4	Informatiebeveiliging.....	8
7.5	Verwerkersovereenkomsten	8
7.6	Privacy by design	8
8.	Bewustzijn en communicatie	9
9.	Planning en controle.....	9
10.	Naleving	9
11.	Vaststelling	10

1. Inleiding

Binnen PMLW wordt gewerkt met persoonsgegevens. Dat gebeurt om als organisatie te kunnen functioneren. Persoonsgegevens hebben wij nodig om de ondernemers op Lage Weide te kunnen bedienen en voor de interne bedrijfsvoering van het bureau.

Iedereen die zijn of haar gegevens aan PMLW toevertrouwt, moet er op kunnen rekenen dat PMLW daar veilig en zorgvuldig mee omgaat. Vanuit onze waarden als werkstichting voor Lage Weide vinden wij dit belangrijk. Bovendien zijn wij aan wettelijke voorschriften gebonden omtrent de privacy en verwerking van persoonsgegevens. Er staan hoge boetes op overtreding.

Nieuwe technologische ontwikkelingen zijn van invloed op de eisen aan de bescherming van gegevens en privacy. Bovendien kunnen persoonsgegevens die wij bewaren en verwerken door een aanval, een vergissing, een natuurverschijnsel (bijv. overstroming of brand door bliksem) worden bedreigd. Dit kan leiden tot het niet beschikbaar zijn van de gegevens, incorrecte administraties, het uitlekken van gegevens en andere ongewenste situaties.

Deze ontwikkelingen en bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om risico's tot een aanvaardbaar niveau te reduceren. PMLW is zich hier van bewust en spant zich in om de privacy te waarborgen, onder andere door maatregelen te treffen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

In dit privacybeleid worden de uitgangspunten en maatregelen die PMLW heeft genomen nader uitgewerkt en inzichtelijk gemaakt hoe deze in de praktijk worden toegepast.

2. Definities

Het is belangrijk een goed begrip te hebben van wat persoonsgegevens zijn (volgens de wet) en welke andere begrippen van belang zijn op het gebied van privacy en gegevensbescherming. Onderstaand daarom de definities inclusief enkele voorbeelden.

Term	Betekenis	Voorbeelden
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.	Directe persoonsgegevens (feiten): Voornaam/achternaam, geboortedatum, adresgegevens, geslacht, identificatienummer/code, vingerafdruk, foto, IQ, etc. Indirecte persoonsgegevens (herleidbare feiten): Scholingsresultaten, locatiegegevens, IP adres, arbeidsgegevens etc.
Bijzonder persoonsgegevens	Gevoelige persoonsgegevens, die door de wetgever extra zijn beschermd.	Ras, godsdienst, gezondheid, politieke overtuiging, seksuele geaardheid, lidmaatschap vakbond, strafrechtelijk verleden
Verwerking	Elke handeling of geheel van handelingen met betrekking tot een persoonsgegeven	Verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, doorsturen, verspreiden, ter beschikking stellen, samenbrengen, koppelen, wissen, vernietigen.
Betrokkene	Een individueel en natuurlijk persoon op wie bepaalde persoonsgegevens betrekking hebben, dan wel van wie bepaalde persoonsgegevens worden verwerkt.	Medewerkers, vertegenwoordigers van de leden, scholieren, ouders
Verwerkingsverantwoordelijke	De natuurlijke of rechtspersoon die het doel en de middelen voor verwerking van persoonsgegevens vaststelt.	Directeur-bestuurder van de werkstichting

Verwerker	Een natuurlijke of rechtspersoon aan wie de verantwoordelijke enige vorm van verwerking van persoonsgegevens heeft uitbesteed. NB. Bij een externe verwerker is de verantwoordelijke nog steeds degene die het doel voor verwerking vaststelt.	Clouddiensten, administratieve dienst
Derde	De natuurlijke of rechtspersoon, die geen betrokkenen, verantwoordelijke of bewerker is, of op enige manier onder gezag van een verantwoordelijke of bewerker valt, maar wel gemachtigd is de gegevens te verwerken. NB. Dit is niet in alle gevallen hetzelfde als een gebruiker/ontvanger van een persoonsgegeven, in welk geval wel sprake kan zijn van een gezagsverhouding.	Samenwerkingspartner, UWV, belastingdienst
Toestemming	Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling een hem betreffende verwerking van persoonsgegevens aanvaardt.	
Kind	In AVG-verband: iedere persoon onder de 16 jaar.	
Doel van de verwerking	Een precieze en duidelijke omschrijving van een doel of verschillende samenhangende doeleinden, waarmee de verantwoordelijke tot uitdrukking brengt waarvoor hij de persoonsgegevens verwerkt. NB. Deze doeleinden dienen voorafgaand aan verwerking te worden vastgesteld en bekendgemaakt.	Ledenadministratie, salarisverwerking
Privacy Impact Assessment	Een tool welke helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.	
Privacy by design	Het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij stelselmatig aandacht wordt besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens. NB. Het idee is dat bij uitvoering van een Privacy Impact Assessment (PIA) de resultaten daarvan worden meegewogen in de ontwikkelingen van de te nemen maatregelen en procedures voor verwerking van persoonsgegevens.	

3. Doel en reikwijdte

PMLW geeft middels dit beleid een duidelijke richting aan privacy en laat zien hoe zij de privacy waarborgt, beschermt en handhaaft. Het privacybeleid is erop gericht om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren, waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen (o.a. ILW leden en medewerkers) wordt gerespecteerd en PMLW voldoet aan relevante wet- en regelgeving.

Dit beleid is van toepassing op de hele organisatie: alle medewerkers, tijdelijk personeel en andere personen die een rol spelen binnen PMLW. En het is van toepassing op alle processen en gegevensverzamelingen van PMLW waar het persoonsgegevens betreft.

Relatie met andere beleidsterreinen

Privacy en gegevensbescherming zijn een integraal onderdeel van informatiebeveiliging. Het Informatiebeveiligingsbeleid van PMLW beschrijft hoe dit binnen PMLW is ingericht en welke implicaties die heeft voor beveiliging van persoonsgegevens. Er wordt dan ook nadrukkelijk verwezen naar het Informatiebeveiligingsbeleid in samenhang met dit privacybeleid.

Privacybeleid heeft ook met andere beleidsgebieden raakvlakken, te weten:

- Algemeen veiligheids- en beveiligingsbeleid: met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en –beveiliging, crisismanagement, huisvesting en ongevallen;
- IT-beleid: met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid: met als aandachtsgebieden in- en uitstroom van medewerkers en vertrouwensfuncties.

4. Wet- en regelgeving

De wettelijke kaders die van toepassing zijn op het privacybeleid:

- de Algemene Verordening Gegevensbescherming (AVG)^{1 2}
- de Uitvoeringswet Algemene Verordening Gegevensbescherming³

5. Uitgangspunten

PMLW gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Wij gaan daarom risico-gebaseerd te werk en zorgen dat dit aantoonbaar is (accountability), zodat indien nodig of wenselijk verantwoording kan worden afgelegd aan belanghebbenden en betrokkenen.

PMLW hanteert daarbij de volgende uitgangspunten:

Rechtmatigheid, behoorlijkheid, transparantie

Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.

Grondslag en doelbinding

PMLW zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtmatige grondslag verwerkt.

Dataminimalisatie

PMLW verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. PMLW streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

¹ <http://wetten.overheid.nl/BWBR0011468/2017-03-10>

² <https://www.legalintelligence.com/documents/18208689?srcfrm=basic+search&docindex=1&stext=Privacyverordening&rid=32bbc236-f2d7-4bd6-8193-45d63bed52f3>

³ <https://www.internetconsultatie.nl/uitvoeringswetavg>

Opslagbeperking

Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de taken van PMLW goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven.

Integriteit en vertrouwelijkheid

PMLW gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen die daartoe bevoegd zijn en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij zorgt PMLW voor passende beveiliging van persoonsgegevens. Deze beveiliging is vastgelegd in het Informatiebeveiligingsbeleid.

Delen met derden

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt PMLW afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. PMLW controleert deze afspraken regelmatig.

Rechten van betrokkenen

PMLW honoreert alle rechten van betrokkenen.

6. Organisatie van privacy binnen PMLW

De stichting PMLW heeft als organisatie uit hoofde van haar rechtspersoonlijkheid verantwoordelijkheden met betrekking tot privacy.

Binnen PMLW zijn deze verantwoordelijkheden inzake privacy georganiseerd op drie niveaus:

1. Richtinggevend (strategisch)
2. Sturend (tactisch)
3. Uitvoerend (operationeel)

6.1 Richtinggevend

Eindverantwoordelijke: De directeur-bestuurder is eindverantwoordelijk binnen PMLW en stelt het beleid en de maatregelen vast op het gebied van privacy en gegevensbescherming.

6.2 Sturend

Privacy Officer: De Privacy Officer heeft binnen PMLW de taak om beleid voor te bereiden, advies te geven en vragen te beantwoorden inzake de toepassing en naleving van de privacywetgeving. De Privacy Officer zorgt tevens voor het afhandelen van incidenten en datalekken conform de wettelijke voorschriften en de procedure die hiervoor is vastgelegd binnen PMLW. Dit valt onder de taken van de Communicatie- en communitymanager.

6.3 Uitvoerend

Projectleiders: Naleving van het privacybeleid is onderdeel van de integrale bedrijfsvoering. Iedere projectleider heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat de collega's binnen zijn team op de hoogte zijn van het privacybeleid;
- toe te zien op de naleving van het privacybeleid door de medewerkers, waarbij hij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;

- als aanspreekpunt beschikbaar te zijn voor privacygerelateerde onderwerpen.

De projectleider wordt in zijn/haar taak ondersteund door de Privacy Officer.

Medewerker: Alle medewerkers hebben een verantwoordelijkheid inzake privacy en gegevensbescherming in hun dagelijkse werkzaamheden. Zij dienen op de hoogte te zijn van in de inhoud van het privacybeleid en zich bewust te zijn van de privacygerelateerde onderdelen van hun werkzaamheden. Van medewerkers wordt verwacht actief betrokken te zijn bij privacy en gegevensbescherming. Dit kan door mogelijke nieuwe, nog niet geregistreerde verwerkingen van persoonsgegevens door te geven aan de Privacy Officer, door alert te zijn en melding te maken van mogelijke beveiligingsincidenten of datalekken.

Verder zijn er een aantal beschreven verantwoordelijkheden die onder andere zijn opgenomen in bijvoorbeeld het 'Aanvaardbaar gebruik van bedrijfsmiddelen', en in de diverse 'Werkafspraken' rondom privacy. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren. Voor vragen over privacy en gegevensbescherming kan de Privacy Officer benaderd worden.

7. Verplichtingen en waarborgen

Binnen PMLW zijn de verplichtingen inzake registratie onder andere geborgd door gepaste softwaretools in te zetten. Bovendien zijn technische en organisatorische maatregelen getroffen om het zorgvuldig en veilig omgaan met persoonsgegevens te waarborgen.

7.1 Register verwerkingen

Het hebben van een register van verwerkingen is een verplichting vanuit de AVG. PMLW heeft zo'n register en hierin zijn alle verwerkingen van persoonsgegevens die binnen PMLW plaatsvinden opgenomen. Doel is om inzichtelijk te hebben wie, waar, waarom en hoelang er met persoonsgegevens wordt gewerkt. Het register mag op verzoek worden ingezien door de toezichthouder, de Autoriteit Persoonsgegevens.

Bij PMLW wordt gebruik gemaakt van een spreadsheet in Sharepoint voor deze registratie. Het vullen en onderhouden van de registraties wordt verzorgd door de Privacy Officer in samenwerking met een aantal medewerkers die op verschillende beleidsterreinen binnen PMLW actief zijn.

In de 'Werkafspraken Privacy: Verwerkingsregister' staat toegelicht welke afwegingen gemaakt moeten worden om te bepalen of er sprake is van een nieuwe verwerking en welke stappen genomen moeten worden bij invoering/aanpassing/verwijdering.

Tevens is in het document 'Werkafspraken Privacy: Bewaartermijnen' een richtlijn opgenomen om de bewaartermijn van persoonsgegevens te bepalen wanneer daar geen wettelijke termijn voor is vastgesteld.

7.2 Protocol privacy-incidenten en datalekken

Er is een wettelijke verplichting tot het melden van datalekken die persoonsgegevens bevatten aan de Autoriteit Persoonsgegevens, "tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen."

PMLW heeft een protocol opgezet voor het geval er (mogelijk) sprake is van een datalek. Iedere medewerker van PMLW moet hiervan op de hoogte zijn en altijd een (mogelijk) datalek onmiddellijk melden bij de Privacy Officer.

Aangezien het ook verplicht is een register bij te houden van incidenten en datalekken, is de spreadsheet in Sharepoint zodanig ingericht, dat deze registratie hierin plaatsvindt.

7.3 Rechten van betrokkenen

Het is wettelijk bepaald dat iedereen recht heeft op inzage, (laten) wijzigen of verwijderen van zijn/haar persoonsgegevens. Om transparant te zijn naar de personen die hun gegevens aan PMLW toevertrouwen, zijn er verschillende mogelijkheden ingericht om dit te faciliteren. Zo wordt aan bezoekers van de website duidelijk gemaakt in de Privacyverklaring, wat er met hun gegevens gebeurt. Bovendien kunnen ILW leden, medewerkers en andere betrokkenen inzage in hun gegevens opvragen. Er is een procedure opgezet ('Werkafspraken Privacy: Rechten van betrokkenen') waardoor een verzoek wat binnenkomt binnen de wettelijk bepaalde termijn en adequaat wordt behandeld⁴.

7.4 Informatiebeveiliging

In het PMLW Informatiebeveiligingsbeleid is vastgelegd hoe PMLW persoonsgegevens behandelt om de veiligheid en integriteit van deze gegevens te waarborgen. Onderdeel van informatiebeveiliging is de bijlage "Informatiestromen- en autorisatiematrix" waarin de primaire en secundaire informatiestromen zijn geïdentificeerd en geclassificeerd, en waarin is vastgelegd wie ervoor verantwoordelijk is, wie toegang heeft tot de gegevens en met welke rechten. Deze bijlage is een belangrijke onderlegger die wordt gebruikt om overzicht te hebben van de in gebruik zijnde persoonsgegevens en is daarom tevens een referentie voor het vullen en beheren van het verwerkingsregister. Om de actualiteit te waarborgen vindt regelmatige herziening van deze bijlage plaats.

7.5 Verwerkersovereenkomsten

PMLW maakt voor sommige van haar diensten gebruik van externe organisaties/leveranciers. Als het voor het uitvoeren van dergelijke diensten nodig is dat persoonsgegevens vanuit PMLW worden aangeleverd en (tijdelijk) gebruikt door een externe partij, wordt contractueel vastgelegd hoe de uitwisseling, de verwerking, het opslaan en het weer verwijderen is georganiseerd, beveiligd en geborgd. Er zijn wettelijke voorwaarden aan deze overeenkomsten gesteld. PMLW hanteert strikt deze voorwaarden en evalueert regelmatig of de overeenkomsten nog afdoende zijn.

7.6 Privacy by design

Privacy by design houdt in dat er bij PMLW al in de beginfase van de ontwikkeling van nieuwe producten en diensten aandacht wordt besteedt aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Daarbij wordt ook rekening gehouden met dataminimalisatie: wij verzamelen en verwerken zo min mogelijk persoonsgegevens, alleen die gegevens die noodzakelijk zijn voor het doel van de verwerking. Door de privacyrisico's van een nieuw product of nieuwe dienst al in een vroegtijdig stadium te onderkennen, is de kans dat er later alsnog mogelijk tijdrovend en kostbaar aanpassingen gemaakt moeten worden klein. Op deze manier kunnen wij een

⁴ Streven is om in de toekomst een portaal in te richten waar betrokkenen zelf na inloggen kunnen bekijken, wijzigen en verzoek tot verwijdering doen. Dit vergemakkelijkt het proces voor zowel betrokkenen als voor de interne organisatie.

zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen. De Privacy Officer kan desgevraagd adviseren in het ontwikkelproces.

8. Bewustzijn en communicatie

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het privacybeleid zijn regelmatig terugkerende bewustwordingscampagnes. Verhoging van het privacy-bewustzijn is een gezamenlijke verantwoordelijkheid van de directeur-bestuurder en de Privacy Officer.

9. Planning en controle

Dit privacybeleid wordt minimaal elke drie jaar, of zodra zich belangrijke wijzigingen voordoen,⁵ getoetst en bijgesteld in opdracht van de directie. Hierbij wordt rekening gehouden met:

- de status van het privacybeleid als geheel (beleid, organisatie, risico's);
- de actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Het gaat hier om een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van technologie, wet- en regelgeving en andere relevante onderwerpen in meegenomen.

10. Naleving

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Het maakt daarom ook deel uit van de PEB-cyclus. Verder wordt er actief aandacht besteed aan privacy bij de aanstelling, met periodieke bewustwordingscampagnes, etcetera.

⁵ In het privacybeleid worden dezelfde termijnen gehanteerd als in het informatiebeveiligingsbeleid.

11. Vaststelling

Dit privacybeleid is in werking getreden na vaststelling door de directie, waarbij de RvC en het team van de werkstichting vooraf advies hebben uitgebracht. De directie communiceert het privacybeleid naar alle medewerkers, zodat bekendheid is geborgd en het belang ervan wordt onderschreven.

Aanpassingen van dit beleid worden aangekondigd via het PMLW-intranet. De meest actuele versie van het beleid is daar ook te vinden.

Aldus vastgesteld op 20 oktober 2022