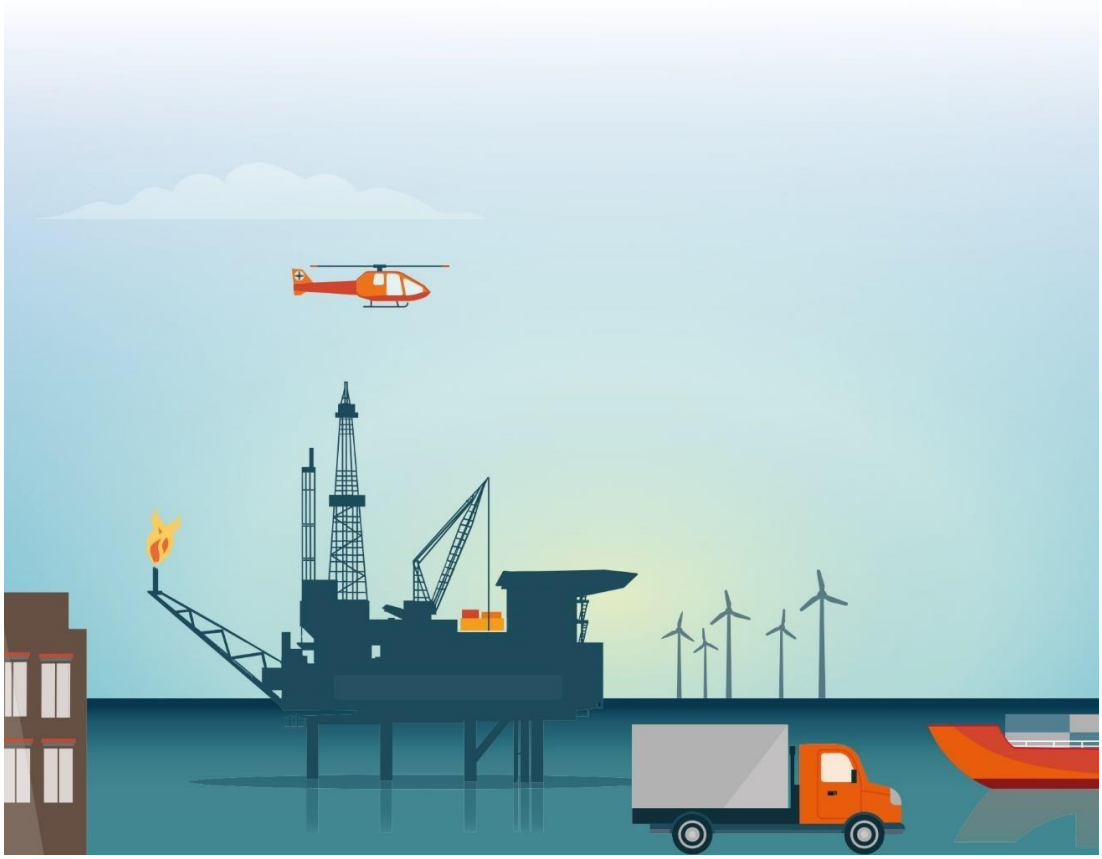
DPIA 4.2 MediWerk B.V.



Versie 4.2 – December 2025
Classificatie: C1-Openbaar
Goedkeuring: Peter Mijnster
Uitvoering: Katja van Mil, Jeanet de Zeeuw, Peter Mijnster

Welkom bij MediWerk

We zijn hier om werkgevers en werknemers te ondersteunen bij het optimaliseren van gezondheid, veiligheid en duurzame inzetbaarheid. Bij MediWerk B.V. (hierna MediWerk) behandelen we persoonsgegevens met de grootst mogelijke zorg en respect voor privacy. Onze Functionaris Gegevensbescherming zorgt ervoor dat we voldoen aan alle geldende wet- en regelgeving, waaronder de AVG. We verzamelen alleen gegevens die nodig zijn voor het uitvoeren van onze taken, inclusief de wettelijke verplichtingen.

Contents

1 | Doel en Reikwijdte

MediWerk verwerkt in het kader van haar dienstverlening persoonsgegevens, waaronder bijzondere persoonsgegevens, in het bijzonder gezondheidsgegevens. Gelet op de aard, omvang, context en doeleinden van deze verwerkingen is deze Data Protection Impact Assessment (DPIA) opgesteld om de verwerking van persoonsgegevens systematisch te beoordelen, de risico's voor betrokkenen inzichtelijk te maken en vast te leggen welke maatregelen worden getroffen om die risico's te beperken. Deze DPIA ondersteunt daarmee zowel de naleving van de AVG als de bredere inrichting van kwaliteit, informatiebeveiliging en privacy binnen MediWerk.

De DPIA ziet primair op de verwerkingen die samenhangen met arbodienstverlening, verzuimbegeleiding, re-integratie, preventieve dienstverlening, PAGO/PMO, medische keuringen, dossiervoering en de uitwisseling van persoonsgegevens in het kader van deze dienstverlening. Daarnaast vallen ook ondersteunende processen binnen scope, voor zover deze relevant zijn voor de rechten en vrijheden van betrokkenen, zoals intake-, contact- en planningsprocessen.

Binnen deze reikwijdte kunnen verschillende categorieën betrokkenen voorkomen, waaronder werknemers, medewerkers van opdrachtgevers, ex-werknemers, deelnemers aan onderzoeken of keuringen, particulieren, contactpersonen bij klanten, websitebezoekers en andere natuurlijke personen van wie MediWerk in het kader van haar dienstverlening persoonsgegevens verwerkt. Het zwaartepunt van deze DPIA ligt bij de verwerkingen binnen de arbodienstverlening en aanverwante medische dienstverlening, omdat daar de grootste gevoeligheid en impact voor betrokkenen ligt.

Deze DPIA staat niet op zichzelf, maar hangt samen met onder meer het verwerkingsregister, het risicomanagementregister, leveranciersbeoordelingen, incidentopvolging en de periodieke directiebeoordeling binnen het managementsysteem van MediWerk. Het document dient daarmee zowel als intern sturings- en verantwoordingsdocument als, waar passend, als extern deelbaar document.

2 | Soorten Persoonsgegevensverwerking door MediWerk

MediWerk verwerkt persoonsgegevens in verschillende vormen en contexten binnen haar dienstverlening. Het gaat daarbij om verwerkingen die nodig zijn voor arbodienstverlening, verzuim- en re-integratiebegeleiding, preventieve dienstverlening, PAGO/PMO, medische keuringen, dossiervoering, communicatie met betrokkenen en opdrachtgevers en ondersteunende processen zoals planning, intake en contactverzoeken.

Afhankelijk van het type dienstverlening verwerkt MediWerk onder meer identificatiegegevens, contactgegevens, werkgever-, functie- en afdelingsgegevens, plannings- en afspraakgegevens, dossier- en correspondentiegegevens, verzuim- en re-integratiegegevens, onderzoeks- en keuringsgegevens en gezondheidsgegevens. Waar dit wettelijk of operationeel noodzakelijk is, verwerkt MediWerk ook aanvullende identificerende gegevens, waaronder het burgerservicenummer. In incidentele gevallen kunnen daarbij ook gegevens van identiteitsdocumenten worden verwerkt, voor zover dat nodig is binnen de betreffende verwerking.

Bijzondere persoonsgegevens, in het bijzonder gezondheidsgegevens, nemen binnen de dienstverlening van MediWerk een centrale plaats in. Deze gegevens worden alleen verwerkt voor zover dat nodig is binnen de uitvoering van de dienstverlening en met passende waarborgen, waaronder beroepsmatige geheimhouding, toegangsbeperking en beveiligingsmaatregelen.

De juridische basis verschilt per verwerking en doel. In de praktijk gaat het met name om verwerking in het kader van wettelijke verplichtingen, de uitvoering van dienstverlening en overeenkomsten, en waar relevant andere toepasselijke grondslagen en uitzonderingsgronden onder de AVG en de Uitvoeringswet AVG. Voor gezondheidsgegevens geldt dat verwerking alleen plaatsvindt voor zover daarvoor een geldige wettelijke basis en passende waarborgen aanwezig zijn. MediWerk maakt geen gebruik van geautomatiseerde besluitvorming met significante gevolgen voor betrokkenen zonder menselijke tussenkomst.

De verstrekking van persoonsgegevens aan derden of ontvangers vindt uitsluitend plaats voor zover dat nodig is binnen de dienstverlening, op grond van een wettelijke verplichting of binnen andere toepasselijke juridische kaders. Daarbij hanteert MediWerk passende afspraken en waarborgen. Persoonsgegevens worden niet langer bewaard dan nodig is voor het doel van de verwerking of zolang als wet- en regelgeving dit vereisen. De nadere uitwerking van ontvangers en bewaartermijnen is opgenomen in de onderliggende privacydocumentatie en, waar relevant, in de operationele registraties van MediWerk.

3 | Noodzaak en Proportionaliteit van de Verwerking

MediWerk verwerkt persoonsgegevens alleen voor zover dat nodig is voor de uitvoering van haar dienstverlening en de daarmee samenhangende ondersteunende processen. Daarbij wordt steeds beoordeeld of het doel van de verwerking niet op een minder ingrijpende manier kan worden bereikt, of met minder persoonsgegevens kan worden volstaan en of de verwerking in verhouding staat tot het doel waarvoor deze plaatsvindt. Dit sluit aan bij de kern van een DPIA zoals bedoeld in artikel 35 AVG.

Gelet op de aard van de dienstverlening is verwerking van medische en arbeidsgerelateerde persoonsgegevens in veel gevallen noodzakelijk. Zonder deze gegevens kan MediWerk haar taken op het gebied van arbodienstverlening, medische keuringen, verzuimbegeleiding, re-integratie en preventieve dienstverlening niet zorgvuldig uitvoeren. Tegelijkertijd brengt deze verwerking een duidelijke inbreuk op de persoonlijke levenssfeer van betrokkenen met zich mee. Daarom beperkt MediWerk de verwerking tot gegevens die nodig zijn voor het specifieke doel, wordt toegang beperkt tot functionarissen die de gegevens voor hun werk nodig hebben en worden passende organisatorische en technische maatregelen toegepast.

MediWerk acht de verwerkingen waarop deze DPIA ziet noodzakelijk en proportioneel, gelet op het doel, de context en de getroffen waarborgen. Die beoordeling wordt periodiek opnieuw bezien, onder meer bij wijzigingen in processen, systemen, gegevensstromen, wet- en regelgeving of risico's.

4 | Risico's voor de Verwerking

De verwerking van persoonsgegevens binnen MediWerk brengt risico's met zich mee voor de rechten en vrijheden van betrokkenen. Deze risico's zijn in het bijzonder relevant bij de verwerking van gezondheidsgegevens, verzuim- en re-integratiegegevens, onderzoeks- en keuringsgegevens en dossiergegevens, omdat verlies van vertrouwelijkheid, onjuiste verwerking of ongeautoriseerde beschikbaarheid van deze gegevens ingrijpende gevolgen kan hebben voor de persoonlijke levenssfeer en rechtspositie van betrokkenen.

MediWerk onderkent met name risico's ten aanzien van ongeautoriseerde toegang tot persoonsgegevens, onjuiste verwerking of koppeling van gegevens aan een onjuist dossier,

onbedoelde openbaarmaking, verlies van gegevens of bedrijfsmiddelen, onjuiste of onvolledige dossiervoering, onvoldoende zorgvuldige verwijdering of bewaarbeheersing en belemmeringen in de transparantie of uitoefening van rechten door betrokkenen. Deze risico's kunnen voortkomen uit menselijke fouten, onzorgvuldige verwerking, systeemfouten, technische kwetsbaarheden, social engineering, phishing, malware, ransomware, onjuiste autorisaties, onveilige opslag en onjuiste verzending of uitwisseling van gegevens.

Als deze risico's zich verwezenlijken, kan dit leiden tot ongewenste kennisname van medische of arbeidsgerelateerde gegevens, aantasting van de persoonlijke levenssfeer, onjuiste verwerking van gegevens in het dossier van een betrokkene, beperkingen in de uitoefening van privacyrechten, verlies van vertrouwen en in voorkomende gevallen materiële of immateriële schade. MediWerk beoordeelt deze risico's op een vaste en navolgbare manier en legt de uitkomsten vast in de DPIA-documentatie en de onderliggende risicoregistratie. Waar nodig worden risico's verder opgevolgd binnen de bestaande werkwijze van MediWerk.

Indien uit deze DPIA of een herbeoordeling daarvan blijkt dat een voorgenomen of gewijzigde verwerking een hoog risico voor betrokkenen oplevert dat ondanks aanvullende maatregelen niet voldoende kan worden beperkt, zal MediWerk beoordelen of voorafgaande raadpleging van de Autoriteit Persoonsgegevens noodzakelijk is voordat de betreffende verwerking wordt voortgezet of ingevoerd.

5 | Beveiliging van Persoonsgegevens bij MediWerk

MediWerk treft passende technische, organisatorische en procedurele maatregelen om persoonsgegevens te beveiligen tegen verlies, ongeautoriseerde toegang, onrechtmatige verwerking, ongewenste wijziging en onbevoegde verstrekking. Daarbij wordt rekening gehouden met de aard van de verwerkte gegevens, de gevoeligheid van met name medische en arbeidsgerelateerde informatie en de risico's voor de rechten en vrijheden van betrokkenen.

Tot deze maatregelen behoren onder meer rolgebaseerde autorisaties, periodieke review van toegangsrechten, meervoudige authenticatie, logging en controle op toegang, endpoint- en devicebeheer, lifecycle management van systemen en bedrijfsmiddelen, versleuteling waar passend, back-up- en herstelmaatregelen, patch- en updatemanagement en beveiligde gegevensuitwisseling. Waar gevoelige gegevens worden uitgewisseld, maakt MediWerk gebruik van passende beveiligde communicatiemiddelen.

De beveiligingsmaatregelen van MediWerk sluiten aan op ISO/IEC 27001:2022 en NEN 7510:2024. MediWerk is gecertificeerd volgens ISO/IEC 27001:2022 conform het certificatieschema Arbodiensten. Ook volgt MediWerk actief informatie over dreigingen en kwetsbaarheden via leveranciersinformatie, security bulletins, informatie van het Nationaal Cyber Security Centrum en andere relevante bronnen. Op basis daarvan beoordeelt MediWerk of updates, aanvullende maatregelen of versnelde opvolging nodig zijn.

Toegang tot persoonsgegevens is beperkt tot personen die deze gegevens voor hun werk nodig hebben. Medewerkers, ingehuurde krachten, consultants en andere betrokkenen zijn gebonden aan geheimhouding en krijgen instructie over het zorgvuldig omgaan met persoonsgegevens, informatiebeveiliging en relevante werkwijzen. MediWerk besteedt daarnaast aandacht aan training en bewustwording op het gebied van privacy, veilig werken en het herkennen van incidenten.

Als MediWerk gebruikmaakt van leveranciers en cloudomgevingen, stelt MediWerk ook daar eisen aan beveiliging, continuïteit en zorgvuldige verwerking van persoonsgegevens. Daarbij is aandacht voor de locatie van verwerking en opslag en voor de vraag of persoonsgegevens binnen de Europese context blijven verwerkt. Het uitgangspunt is dat het zwaartepunt van dossierverwerking binnen Nederland ligt. MediWerk beschikt daarnaast over een proces voor het signaleren, beoordelen, escaleren en afhandelen van beveiligingsincidenten en privacy-incidenten. Binnen de verwerkingen waarop deze DPIA betrekking heeft, gebruikt MediWerk geen AI-toepassingen voor geautomatiseerde verwerking of beoordeling van persoonsgegevens.

6 | Belanghebbenden en Documentatie

Bij het uitvoeren, actualiseren en opvolgen van deze DPIA betrekt MediWerk de relevante belanghebbenden die vanuit hun rol, verantwoordelijkheid of betrokkenheid invloed hebben op de verwerking en bescherming van persoonsgegevens. Het gaat daarbij in ieder geval om interne belanghebbenden zoals directie, Functionaris Gegevensbescherming en relevante functionarissen op het gebied van operatie, informatiebeveiliging, governance en kwaliteit, maar ook om externe belanghebbenden zoals opdrachtgevers en werknemers van opdrachtgevers voor zover hun signalen, ervaringen of belangen relevant zijn.

De afstemming vindt plaats via de vaste overlegstructuren van MediWerk, waaronder het governanceteamoverleg, het managementteamoverleg, het overleg van de kerndeskundigen en de directiebeoordeling. Daarnaast gebruikt MediWerk signalen uit de praktijk, zoals klachten, privacyverzoeken, incidenten, auditbevindingen en andere terugkoppelingen, om verwerkingen, risico's en maatregelen opnieuw te beoordelen wanneer daar aanleiding voor is.

In deze DPIA is beoordeeld hoe de belangen, rechten en signalen van betrokkenen worden meegenomen. Gezien de aard van de dienstverlening en de vertrouwelijkheid van medische en arbeidsgerelateerde gegevens gebeurt dit meestal niet via directe individuele raadpleging, maar via signalen, terugkoppeling en bestaande contactkanalen. De Functionaris Gegevensbescherming houdt hierbij onafhankelijk toezicht en ziet erop toe dat de belangen en rechten van betrokkenen worden meegenomen bij de beoordeling en actualisatie van de DPIA.

De DPIA wordt beheerd als formeel document binnen het managementsysteem. MediWerk legt de relevante bevindingen, risico's, maatregelen en opvolgpunten vast en houdt daarbij samenhang met onder meer het verwerkingsregister, het risicomanagementregister, incidentregistraties en leveranciersbeoordelingen. Naast de DPIA stelt MediWerk ook andere privacydocumentatie beschikbaar, waaronder de privacyverklaring en de klachtenprocedure via de website en, waar passend, ter inzage op kantoor of op verzoek.

7 | Verantwoordelijkheid en Opvolging

MediWerk zorgt ervoor dat de uitkomsten, risico's en maatregelen uit deze DPIA worden opgevolgd. Daarbij is duidelijk belegd wie verantwoordelijk is voor beoordeling, besluitvorming, uitvoering, toezicht en herbeoordeling.

Het governanceteam is gezamenlijk verantwoordelijk voor de inhoudelijke beoordeling van de DPIA, de risico's en de maatregelen en beoordeelt ook of actualisatie of aanscherping nodig is. De Functionaris Gegevensbescherming heeft binnen dit proces een coördinerende en onafhankelijke

toezichthoudende rol en ziet erop toe dat relevante risico's, signalen en maatregelen goed in de DPIA worden verwerkt en tijdig binnen de organisatie worden teruggelegd. Het managementteam is verantwoordelijk voor de formele vaststelling van de DPIA en voor besluitvorming over verdere opvolging, prioriteiten, ondersteuning en maatregelen.

De uitvoering van maatregelen en verbeteracties vindt plaats binnen de daarvoor relevante onderdelen van de organisatie. Afhankelijk van het onderwerp kunnen daarbij operationele functionarissen, inhoudelijk deskundigen, proceseigenaren, IT, informatiebeveiliging of andere betrokkenen worden ingezet. De voortgang op relevante risico's, maatregelen en aandachtspunten wordt gevolgd in het governanceteamoverleg, het managementteamoverleg, de directiebeoordeling en, waar nodig, in operationeel overleg.

8 | Periodieke Herbeoordeling en Bijwerking

MediWerk beoordeelt deze DPIA periodiek om te borgen dat de inhoud blijft aansluiten op de feitelijke verwerking van persoonsgegevens, de geldende wet- en regelgeving, de inrichting van de dienstverlening en de actuele risicobeheersing binnen de organisatie. Als uitgangspunt wordt de DPIA ten minste jaarlijks opnieuw beoordeeld en geactualiseerd. Daarnaast wordt de DPIA eerder bijgewerkt indien daar aanleiding toe bestaat, bijvoorbeeld bij wijzigingen in dienstverlening, processen, systemen, medische werkwijzen, gegevensstromen, wet- en regelgeving, leveranciersafhankelijkheden, beveiligingsmaatregelen, incidenten, klachten, privacyverzoeken of auditbevindingen.

Bij een herbeoordeling wordt bezien of de beschreven verwerkingen nog juist zijn, of de benoemde risico's nog aansluiten op de praktijk en of bestaande maatregelen nog passend en aantoonbaar effectief zijn. De uitkomsten van een herbeoordeling kunnen leiden tot aanpassing van risico-inschattingen, maatregelen of onderliggende documentatie. Zo blijft de DPIA actueel en bruikbaar.

9 | Vertrouwelijkheid en Toegang tot de DPIA

MediWerk maakt bij de beschikbaarheid van DPIA-documentatie onderscheid tussen verschillende versies en detailniveaus. Niet alle informatie uit de volledige DPIA is geschikt voor brede interne of externe verspreiding, met name waar het gaat om nadere risico-uitwerkingen, kwetsbaarheden en andere detailinformatie.

Voor interne beheersing en governance beschikt MediWerk over een volledige versie van de DPIA, inclusief de nadere risico-uitwerking en bijbehorende detailinformatie. Daarnaast kan MediWerk een extern deelbare versie van de DPIA beschikbaar stellen aan klanten en andere relevante partijen. Deze versie is bedoeld als verantwoordingsdocument en biedt inzicht in de wijze waarop MediWerk privacyrisico's beoordeelt en persoonsgegevens beschermt, zonder dat daarin automatisch alle interne risico-uitwerkingen, kwetsbaarheden of beheersdetails worden opgenomen.

De nadere risico-uitwerking en overige gevoelige detailinformatie kunnen afzonderlijk worden beheerd, bijvoorbeeld in een appendix of onderliggende documentatie die onderdeel uitmaakt van de interne DPIA-versie. Bij interne of externe beschikbaarstelling wordt steeds de documentversie gebruikt die past bij het doel en de doelgroep. Dit laat onverlet dat MediWerk relevante privacy-informatie publiek beschikbaar stelt via de privacyverklaring en de klachtenprocedure