Beveiligings- en privacybeleid Welder

Versie: November 2026

Beschrijving van:

- De technische inrichting van de Welder applicatie
- Alle privacy maatregelen van Welder
- Resultaten van externe toetsen door onafhankelijke partijen
- Privacy statement

Inhoud

Hoofdstuk 1 | Voorwoord 2
Hoofdstuk 2 | Definities 3
Hoofdstuk 3 | Beleidsmaatregelen 4
Hoofdstuk 4 | Verwerkingsregister 7
Hoofdstuk 5 | Technische Inrichting 13
Hoofdstuk 6 | Data Protection Impact Assessment (DPIA) 17
Hoofdstuk 7 | Penetratie testen 20
Hoofdstuk 8 | Externe toets door De Functionaris 21
Hoofdstuk 9 | Data Processing Addendum / Addendum Verwerkersovereenkomst 41
Hoofdstuk 10 | Privacy Statement 45
Hoofdstuk 11 | Roadmap ISO-certificering 49
Hoofdstuk 12 | Resultaten interne toets 50

Hoofdstuk 1 | **Voorwoord**

Binnen Welder maken we enorm mooie digitale toepassingen voor medewerkers. Met ons platform kunnen medewerkers en leidinggevenden heel eenvoudig ontwikkelgesprekken voeren, direct betrokken worden bij bedrijfsontwikkelingen of E-learnings volgen. Zo dragen we bij aan de persoonlijke ontwikkeling van veel medewerkers.

Om dit te kunnen faciliteren, moeten we veel data opslaan en verwerken. Dat biedt dus vele voordelen, maar brengt ook verantwoordelijkheden met zich mee. We realiseren ons binnen Welder terdege dat bescherming van privacy wellicht de grootste uitdaging van onze organisatie is.

Daarom nemen we flinke maatregelen en doen we er alles aan om te voorkomen dat data in verkeerde handen komt. We kiezen hierbij voor een beleid dat zich allereerst richt op de aantoonbare technische veiligheid. De aantoonbare maatregelen die genomen zijn in de architectuur van onze toepassingen. We zien helaas nog te vaak bureaucratische schijnveiligheid; er zijn uitgebreide handboeken, beleidsstukken en procedures waar medewerkers nauwelijks van op de hoogte zijn. Daarom laten we ook periodiek ons systeem door externen toetsen en streven we naar een ISO certificering eind 2026. Uiteraard hebben we ook de juiste beleidsmaatregelen genomen.

Dit document geeft meer inzicht in het totaalpakket aan maatregelen die Welder neemt rond veiligheid en privacy van data. Alle medewerkers van Welder worden hier uitgebreid in meegenomen. Jaarlijks wordt dit document herzien als vast item in de jaarplannen van Welder.

Zo zorgen we ervoor dat persoonsgegevens bij Welder in veilige handen zijn. Nu en in de toekomst.

Rob Wouters en Maarten Schellekens - eigenaren Welder

Hoofdstuk 2 | **Definities**

AVG | De Algemene verordening gegevensbescherming (AVG) regelt wat er allemaal wel en niet mag met de persoonsgegevens van mensen. Bij elk gebruik van persoonsgegevens geldt dat de privacyinbreuk zo klein mogelijk moet zijn.

Opdrachtgever | De organisatie waar WELDER BV een overeenkomst mee sluit en die gebruik maakt van de software van Welder.

Verwerkingsverantwoordelijke | De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. In een overeenkomst tussen Welder en Opdrachtgever is de Opdrachtgever de verwerkingsverantwoordelijke.

Verwerker | Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. In een overeenkomst tussen Welder en Opdrachtgever is Welder de verwerker.

Eindgebruiker | Medewerkers van een Opdrachtgever die de Welder software gebruikt. Bijvoorbeeld om intern berichten te delen, ontwikkelgesprekken voor te bereiden of een E-learning te doorlopen.

Gesprekscyclus | alle momenten waarop leidinggevenden met medewerkers praten over hun ontwikkeling. Ook wel HR-cyclus of HRM-cyclus genoemd.

Welder software | De digitale toepassing die Welder ontwikkeld heeft voor het binden, boeien, leren en ontwikkelen van medewerkers.

Ontwikkelgesprek | Een gesprek tussen twee Eindgebruikers over bijvoorbeeld tevredenheid, prestaties of ambities. Deze gesprekken kunnen via de Welder software ingepland, voorbereid en vastgelegd worden.

E-learning | Een digitale toepassing binnen de Welder software waarin de Opdrachtgever haar medewerkers (Eindgebruikers) wat wil leren over een bepaald onderwerp.

(1e/2e) Leidinggevende | De Eindgebruiker die hiërarchisch boven een andere Eindgebruiker staat. Deze persoon plant bijvoorbeeld vaak de gesprekken in een Gesprekscyclus.

Koppeling | Het door Welder automatisch overnemen van personeelsdata uit bijvoorbeeld een salarispakket.

Hoofdstuk 3 | **Beleidsmaatregelen**

3.1 Beleidsmaatregelen

In dit beleid is beschreven welke interne maatregelen getroffen worden door Welder in het kader van beveiliging en privacy. Dit beleid wordt periodiek extern getoetst.

Er zijn verschillende documenten beschikbaar rond het beveiligings- en privacybeleid van Welder:

- **Beveiligings- en privacy beleid |** Geldt als bronbestand. De belangrijkste uitgangspunten van Welder zijn hierin vermeld.
- **Privacy statement Welder |** Dit krijgen veel nieuwe gebruikers te zien wanneer ze voor het eerst gebruik maken van de software van Welder. Hierin zijn essentiële punten uit dit Beveiligings- en privacybeleid opgenomen die relevant zijn voor een Eindgebruiker.
- **Verwerkersovereenkomst |** Hierin worden op basis van het Beveiligings- en privacybeleid van Welder specifieke afspraken gemaakt tussen Welder en Opdrachtgever.
- **Algemene Voorwaarden |** Hierin worden randvoorwaarden van een samenwerking tussen Welder en Opdrachtgever vastgelegd.
- **Contracten medewerkers Welder |** Hierin worden onder andere verwachtingen van Welder naar de medewerkers tav beveiliging en privacy vastgelegd.

3.2 Autorisatiemodel

In een autorisatiemodel wordt weergegeven welke medewerkers van Welder welke rechten hebben. In onderstaand autorisatiemodel is weergegeven welke interne/externe stakeholders van Welder toegang hebben tot welke data.

	Gebruikers-gegevens van Eind-gebruikers	Toegang tot database gegevens	Verlenen / aanpassen autorisaties Welder medewerkers	Welder-only functies in Welder software	Beheerders-rechten in Welder software
Development Welder	x	x		x	x
Customer Succes Managers Welder	x			x	x
Overige Welder medewerkers					
Directie Welder	x	x	x	x	x
Eindgebruikers Opdrachtgever	x				
Beheerders Opdrachtgever	x				x

De privacy officer van Welder is ervoor verantwoordelijk dit autorisatiemodel te bewaken, het te signaleren wanneer er afwijkingen ontstaan en waar nodig aanpassingen te doen.

3.3 Data eigenaarschap

Opdrachtgever is eigenaar van de data en is er als zodanig eindverantwoordelijk voor dat Eindgebruikers gewezen worden op rechten rond privacy. Er zijn drie opties in deze:

- Opdrachtgever heeft reeds in haar contracten met medewerkers hierover geïnformeerd;
- Opdrachtgever hanteert een separaat privacy statement dat zij zelf opstellen (eventueel op basis van stramien onderaan dit document);
- Opdrachtgever hanteert een separaat privacy statement dat door Welder beschikbaar wordt gesteld.

Daarnaast sluiten Welder en opdrachtgevers een verwerkersovereenkomst waarin gebruik van data en rechten van gebruikers staan beschreven.

3.4 Rollen en verantwoordelijkheden

Het is belangrijk intern de juiste rolverdeling te kennen rond het beschermen van persoonsgegevens. Hieronder een verdeling van de medewerkers met de verantwoordelijkheden in deze.

Betrokkene(n) Welder	Rol / verantwoordelijkheid
Privacy officer / functionaris gegevensbescherming (2026: Jari van Galen)	Uitvoering van privacybeleid Rapporteren aan directie over naleving privacybeleid. Uitvoering van DPIA eens per 2 jaar
Developers Welder	Beheer en ontwikkeling technische maatregelen rond privacy.
Technisch Specialist Welder	Beheer van koppelingen met personeelsinformatiesystemen en importeren van gebruikersgegevens
Customer Succes Managers Welder	Communicatie naar Opdrachtgevers in kader privacy beleid.
Directie Welder (Rob Wouters, Maarten Schellekens)	Bepalen van het privacybeleid. Eindverantwoordelijk gegevensbescherming.

Alle medewerkers van Welder ontvangen bij indiensttreding een digitale training op het gebied van gegevensbescherming. Daarna ontvangt elke medewerker 1x per jaar een training op het gebied van gegevensbescherming. De inhoud hiervan wordt opgesteld door de privacy officer.

3.5 ICT-gebruik en sociale media

Richtlijnen voor het gebruik van ICT-middelen en sociale media zijn vastgelegd in de arbeidsovereenkomst met elke medewerker van Welder.

3.6 Budget

De directie is ervoor verantwoordelijk dat er voldoende budget beschikbaar wordt gesteld om de maatregelen uit dit beveiligings- en privacybeleid na te leven. Wanneer er onvoldoende budget vrijgemaakt is, dient dit door de privacy officer gecommuniceerd te worden aan de directie.

3.7 Uitwisseling data en documenten

Wanneer er persoonsgegevens van Eindgebruikers van Opdrachtgever aangeleverd worden bij Welder, is het de taak van alle medewerkers ervoor te zorgen dat deze geupload worden via het apart daarvoor ingerichte documentenportaal. De Technisch specialist krijgt een signaal hiervan, kan evalueren of dit de juiste data is en deze verwerken. Zo voorkomen we dat dergelijke persoonsgegevens terecht komen bij mensen waarvoor deze niet bedoeld zijn.

3.8 Toestemming beeldmateriaal

Elke medewerker van Welder mag zelf kiezen om wel of niet gefotografeerd te worden door een professionele fotograaf. Door bewust op de foto te gaan geeft de medewerker toestemming dat het beeldmateriaal ook extern gedeeld / gebruikt kan worden.

3.9 Wachtwoordbeleid

Welder werkt met een Single Sign On beleid via Google. Elke medewerker van Welder wordt bij indiensttreding uitgenodigd hiervan gebruik te maken en een uniek wachtwoord te genereren. Het is niet toegestaan een wachtwoord te hanteren dat persoonlijk onthouden kan worden; er dient gebruik te worden van een password manager, te weten Bitwarden. Aan alle medewerkers van Welder wordt geadviseerd het Google wachtwoord elk kwartaal te wijzigen.

3.10 Evaluatie beleidsmaatregelen

Deze beleidsmaatregelen worden eenmaal per jaar geëvalueerd door de functionaris Gegevensbescherming van Welder en in overleg met directie Welder geüpdatet.

Hoofdstuk 4 | **Verwerkingsregister**

4.1 Activiteiten

Welder onderneemt de volgende activiteiten waarbij gegevens verwerkt worden:

- Klanten die de Welder software gebruiken (4.2)
- Werving / Selectie / Personeelsadministratie (4.3)
- Marketing / Sales / CRM (4.4)
- Financiële administratie (4.5)

Hieronder worden per activiteit vastgelegd wie welke verantwoordelijkheid heeft, welke gegevens verzameld worden met welke motivatie, op welke manier deze verkregen worden en of het gevoelige persoonsgegevens betreft.

4.2 Klanten die de Welder software gebruiken

Hierna is beschreven welke uitgangspunten gehanteerd worden rond de belangrijkste activiteit van Welder: klanten die de Welder software gebruiken.

4.2.1 Verantwoordelijke

Wanneer Welder een contract sluit met een Opdrachtgever om de software van Welder beschikbaar te stellen aan de Eindgebruikers van Opdrachtgever is de Opdrachtgever de verwerkingsverantwoordelijke en Welder de verwerker.

4.2.2 Persoonsgegevens

Per Opdrachtgever wordt bekeken welke persoonsgegevens verzameld moeten worden. Hierbij geldt: liefst zo min mogelijk. Alleen de persoonsgegevens die noodzakelijk zijn voor de dienstverlening worden verzameld. Hieronder een overzicht van de persoonsgegevens die verzameld kunnen worden, inclusief een motivatie waarom deze noodzakelijk zijn.

Persoonsgegevens	Motivatie
Naam	Noodzakelijk om te weten om welke Eindgebruiker het gaat en hem/haar zo te kunnen aanspreken in bijvoorbeeld e-mailverkeer.
E-mail	Noodzakelijk om te kunnen communiceren met Eindgebruikers. Bijvoorbeeld om ze uit te nodigen de software van Welder te gebruiken.
Geboortedatum	Opdrachtgevers kiezen ervoor een ontwikkelgesprek te voeren rond een verjaardag. Er bestaat een setting om het jaartal en leeftijd af te schermen.
Datum in dienst	Noodzakelijk zodat Eindgebruikers uitgenodigd kunnen worden een digitaal inwerkprogramma te volgen of een vragenlijst in te vullen.
Datum uit dienst	Noodzakelijk zodat Eindgebruiker uitgenodigd kunnen worden voor een exit-gesprek of een vragenlijst.
Functie	Noodzakelijk zodat Eindgebruikers kunnen zien welke competenties van een functie verwacht worden of wanneer Opdrachtgever wil segmenteren in bijvoorbeeld een gesprekscyclus of een E-learning en alleen

	Eindgebruikers met een bepaalde functie wil uitnodigen hiervoor.
Afdeling	Noodzakelijk zodat een Opdrachtgever kan segmenteren in bijvoorbeeld een gesprekscyclus of E-learning en alleen Eindgebruikers van een bepaalde afdeling wil uitnodigen hiervoor.
1e Leidinggevende	Noodzakelijk zodat bekend is wie een ontwikkelgesprek met de Eindgebruiker mag voeren en wie inzicht mag hebben in de persoonlijke ontwikkeling van welke Eindgebruikers.
2e Leidinggevende	Noodzakelijk zodat bekend is wie een ontwikkelgesprek met de Eindgebruiker mag voeren en wie inzicht mag hebben in de persoonlijke ontwikkeling van welke Eindgebruikers.
Organisatie	Noodzakelijk zodat bekend is bij welke Organisatie de Eindgebruikers werken.
Salaris	Noodzakelijk zodat de Eindgebruiker met zijn/haar Leidinggevende het salaris kan bespreken tijdens een ontwikkelgesprek. In uitzonderingsgevallen wordt in de synchronisatie met een salarispakket een loonstrook gesynchroniseerd en aan de individuele gebruiker getoond in het dossier in Welder. Het salaris is alleen inzichtelijk voor de betreffende medewerker en diens leidinggevende. Deze informatie wordt niet gedeeld met andere medewerkers binnen de organisatie.
Salarisschaal	Noodzakelijk zodat de Eindgebruiker met zijn/haar Leidinggevende het salaris kan bespreken tijdens een ontwikkelgesprek.
Salaris trede	Noodzakelijk zodat de Eindgebruiker met zijn/haar Leidinggevende het salaris kan bespreken tijdens een ontwikkelgesprek.
Taal	Noodzakelijk zodat helder is in welke taal de Welder software getoond moet worden.
Telefoonnummer	Noodzakelijk voor het functioneren van sommige van onze systeemfunctionaliteiten. Bijvoorbeeld zodat Eindgebruikers elkaar snel telefonisch kunnen bereiken.

Een Opdrachtgever kan ervoor kiezen extra persoonsgegevens uit te vragen aan de Eindgebruiker. Dit zijn dan enkele persoonsgegevens die een medewerker zelf ingeeft en toestemming geeft om ze te verwerken.

4.2.3 Verkrijgen van persoonsgegevens

Welder verkrijgt deze persoonsgegevens op verschillende manieren van Opdrachtgevers.

- De Eindgebruiker vult deze informatie zelf in binnen de Welder software
- De Opdrachtgever levert deze informatie aan bij Welder
- Er wordt een automatische koppeling gelegd met een sofware systeem dat de Opdrachtgever reeds gebruikt

De beste wijze wordt per Opdrachtgever in onderling overleg bepaald.

Wanneer persoonsgegevens aangeleverd worden, gebeurt dit nooit per e-mail, maar via een apart ingerichte online omgeving die binnenkomt bij de Technisch Specialist van Welder. Zo beperken we het risico dat een medewerker per ongeluk een mail doorstuurt.

4.3 Werving / Selectie / Personeelsadministratie

Hierna is beschreven welke uitgangspunten gehanteerd worden rond de werving, selectie en personeelsadministratie. Oftewel alle (mogelijke) medewerkers van Welder.

4.3.1 Verantwoordelijke

Welder is in dit geval verantwoordelijk voor de verwerking van de (persoons)gegevens.

4.3.2 Persoonsgegevens

Van potentiële medewerkers worden enkel naam, CV en e-mailadres en/of telefoonnummer opgeslagen. Het CV om te evalueren of de kandidaat voldoende ervaring heeft voor de in te vullen functie en de contactgegevens om contact op te nemen met de kandidaat. Van huidige medewerkers worden de volgende gegevens verzameld:

Persoonsgegevens	Motivatie
Adres, postcode, woonplaats	Om een brief te kunnen versturen naar het woonadres. En om woon-werkverkeer vast te stellen.
Telefoonnummer	Om contact te kunnen leggen.
Privé e-mailadres	Om per mail te kunnen communiceren zolang het zakelijk mailadres nog niet geactiveerd is of (tijdelijk) niet gebruikt wordt.
BSN	Ter identificatie
IBAN	Om het salaris over te kunnen maken.

4.3.3 Verkrijgen van persoonsgegevens

Welder verkrijgt deze persoonsgegevens door ze op te vragen bij de betreffende (potentiele) medewerker. Deze (potentiele) medewerker geeft toestemming de gegevens te gebruiken.

4.4 Marketing / Sales / CRM

Hierna is beschreven welke uitgangspunten gehanteerd worden rond de Welder activiteiten gericht op marketing en sales.

4.4.1 Verantwoordelijke

Welder is in dit geval verantwoordelijk voor de verwerking van de (persoons)gegevens.

4.4.2 (Persoons)gegevens

De volgende gegevens worden verzameld bij de marketing- en salesactiviteiten van Welder.

(Persoons)gegevens	Motivatie
Websitebezoek	Om het aantal websitebezoekers te kunnen monitoren, op basis van IP-adres.
Vindbaarheid van pagina's	Om de SEO-prestaties te verbeteren
Kliks op advertenties	Om de resultaten van de (Google) Advertenties te kunnen monitoren.
Bedrijfsnaam	Om contact op te kunnen nemen bij een demo-aanvraag
Naam	Om contact op te kunnen nemen bij een demo-aanvraag
Aantal medewerkers	Om te weten om wat voor formaat organisatie het gaat
Telefoonnummer	Om contact op te kunnen nemen bij een demo-aanvraag
E-mailadres	Om contact op te kunnen nemen bij een demo-aanvraag
Functie	Om contact op te kunnen nemen bij een demo-aanvraag
Salarispakket	Om te weten waar we een mogelijke koppeling mee zouden moeten leggen
E-mail / telefonisch verkeer	Om overige Welder collega's te informeren over het contact dat er met deze klant is geweest
Anoniem beeldmateriaal	Voorbeeld en inspiratie voor andere klanten

4.4.3 Verkrijgen van persoonsgegevens

Websitebezoek, vindbaarheid en kliks op advertenties worden automatisch gegenereerd door software programma's (Google Analytics, Semrush, Google Ads). Dat is vooralsnog anoniem.
Wanneer een demo-aanvraag gepland wordt of een contactformulier ingevuld wordt, wordt er naar enkele contactgegevens gevraagd. Ook wordt hier gewezen op dit privacy- en beveiligingsbeleid. Al het contact met potentiele nieuwe klanten, wordt opgeslagen in het CRM pakket van Welder (HubSpot).

4.5 Financiële administratie

Hierna is beschreven welke uitgangspunten gehanteerd worden rond de Welder activiteiten gericht op financiele administratie.

4.5.1 (Persoons)gegevens

De volgende gegevens worden verzameld bij de financiele administratie van Welder.

(Persoons)gegevens	Motivatie
IBAN leverancier	Om geld over te kunnen maken naar onze leveranciers
IBAN klant	Voor een eventuele creditfactuur
Kostenplaats klant	Voor de administratie van klanten
Adresgegevens klant	Voor eventuele communicatie per post
E-mailadres klant	Voor communicatie op administratief vlak
Betalingen klant	Voor eventuele betaalherinneringen

4.5.2 Verkrijgen van persoonsgegevens

De klantgegevens worden opgevraagd bij de klant. Hierbij wordt aangegeven waar deze gegevens noodzakelijk voor zijn. Alle verkregen gegevens worden vastgelegd in het facturatieprogramma van Welder (WeFact).
Betaalgegevens worden automatisch verwerkt door het administratieprogramma van Welder (Exact).

4.6 Gevoelige persoonsgegevens

De persoonsgegevens die Welder verzamelt vallen onder de 'gewone persoonsgegevens'. De salarisgerelateerde persoonsgegevens kunnen als 'gevoelige persoonsgegevens' omschreven worden en Welder maakt haar medewerkers ervan bewust dat extra discreet omgegaan wordt met deze persoonsgegevens.

4.7 Subverwerkers

Welder heeft momenteel twee subverwerkers (Hetzner te Duitsland als hosting partner en OVH in Frankrijk als Back-up hosting provider) en garandeert dat dergelijke subverwerkers een soortgelijk verwerkingsregister vastleggen met contactgegevens.

4.8 Rechtmatigheid van verwerking

Er worden in de AVG zes grondslagen genoemd die de rechtmatigheid beschrijven van het verwerken van persoonsgegevens:

1. U heeft toestemmming van de persoon om wie het gaat
2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren
3. Het is noodzakelijk om gegevens te verwerken omdat u dit wettelijk verplicht bent
4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen
5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen
6. Het is noodzakelijk om gegevens te verwerken om uw gerechtvaardigde belang te behartigen

De software van Welder is dusdanig op verschillende manieren in te zetten binnen een organisatie dat iedere opdrachtgever zelf de juiste grondslag moet bepalen.
Er zijn meerdere grondslagen die van toepassing kunnen zijn om persoonsgegevens te verwerken. Dit is mede afhankelijk van de afgenomen modules en bepaalde keuzes die gemaakt worden in de te verwerken persoonsgegevens. Het gebruik van bedrijfssoftware wordt meestal onder Grondslag 6, gerechtvaardigd belang opgenomen. Mits de organisatie in het kader van dataminimalisatie altijd kritisch op de gegevens die worden verwerkt.

Interne communicatie: Grondslag 6, gerechtvaardigd belang.
De bedrijfssoftware wordt ingezet als intranet binnen de organisatie voor een efficiënte communicatie vanuit de organisatie naar de medewerkers en de medewerkers onderling. Om dit goed te faciliteren zijn de basisgegevens noodzakelijk om te verwerken.

Leren en Ontwikkelen: Grondslag 6, gerechtvaardigd belang/ Grondslag 2, uitvoering overeenkomst.
Voor Leren en Ontwikkelen kan de organisatie gebruik maken van meerdere features om kennis, informatie en ontwikkeling beschikbaar te stellen aan medewerkers. Afhankelijk van de invulling kan de grondslag verschillen. Maar overall gezien heeft de organisatie een gerechtvaardigd belang om kennis en informatie beschikbaar te stellen aan medewerkers om het werk goed uit te kunnen voeren. In het geval van verplichte trainingen die vereist zijn voor het uitoefenen van de functie is ook grondslag 2 een gerechtvaardigde grondslag voor het verwerken van persoonsgegevens.

Onboarding: Grondslag 6, gerechtvaardigd belang/ Grondslag 3, wettelijke verplichting.
In het geval van een onboarding heeft een organisatie een zwaarwegend belang om een goede onboarding beschikbaar te stellen voor alle nieuwe medewerkers. Dit belang weegt zwaarder dan de lichte inbreuk op privacy indien er niet meer gegevens dan noodzakelijk worden verwerkt. Indien Welder ook wordt ingezet voor het opvragen van wettelijk verplichte documenten is ook grondslag 3 aan de orde.

Medewerkersonderzoeken: Grondslag 6, gerechtvaardigd belang
Als werkgever heeft de organisatie een gerechtvaardigd belang om de werkomgeving, tevredenheid en vitaliteit van de medewerkers te monitoren en te verbeteren. In dit geval is het vooral van belang wat de reden van het onderzoek is en welke reden de organisatie heeft om dit onderzoek uit te voeren. Daarnaast kan deze module ook gebruikt worden voor het inzetten van formulieren die vereist zijn voor het (efficiënt) uitvoeren van de werkzaamheden waar ook grondslag 6 van toepassing is.

Gesprekken voeren: Grondslag 6, gerechtvaardigd belang/ Grondslag 2, uitvoeren overeenkomst/ Grondslag 3, wettelijke verplichting.
De organisatie zet de bedrijfssoftware in voor het voeren van ontwikkelgesprekken. Daarmee heeft de organisatie een gerechtvaardigd belang om de prestaties van medewerkers te beoordelen, te monitoren en te begeleiden in zijn/haar ontwikkeling. Indirect kunnen deze gesprekken ook nodig zijn voor de uitvoering van de overeenkomst. Voor het bepalen van promotie, opleidingen en/of salarisgroei.
In sommige sectoren is het wettelijk verplicht om gesprekken te voeren en dan is ook grondslag 3 aan de orde.

Welder faciliteert ook grondslag 1, toestemming. Door de inzet van een Pop-up met een link naar het interne privacy statement van de organisatie kan de werknemer akkoord gaan en toestemming geven voor het verwerken van persoonsgegevens. Vanwege gezagsverhouding tussen werkgever en werknemer kan dit een complexe grondslag zijn en zal er door de organisatie goed beargumenteerd moeten worden dat medewerkers de vrije keuze hebben om wel of geen gebruik te maken van de software zonder gevolgen voor de arbeidsrelatie.

De Eindgebruiker heeft altijd het recht deze toestemming in te trekken, dat kan met één mail naar info@welder.nl. Dit wordt toegelicht in het privacy statement.

Hoofdstuk 5 | **Technische Inrichting**

5.1 Architectuur van dienst/applicatie

Welder levert een cloudoplossing om te investeren in het leren, ontwikkelen, binden en boeien van medewerkers.

5.2 Aantal actieve gebruikers

Op 1 januari 2026 bedraagt het aantal gebruikers van Welder ca. 130.000.

5.3 Privacy by Design en Privacy by Default

Privacy by design en privacy by default zijn twee verplichte uitgangspunten uit de Algemene Verordening Gegevensbescherming (AVG). Bij privacy by design gaat het om aandacht voor gegevensbescherming in de ontwerpfase van een product of dienst. Privacy by default houdt in dat de standaardinstellingen zo privacy-vriendelijk mogelijk moeten zijn.
De developmentafdeling van Welder wordt periodiek getraind in deze uitgangspunten en bij elke ontwikkeling worden deze principes toegepast.

5.4 Beëindiging / faillissement

Wanneer Welder om wat voor reden dan ook ophoudt te bestaan, zal opdrachtgever hierover tijdig geïnformeerd worden door opdrachtnemer. Opdrachtnemer is in dat geval verplicht de software ten minste 1 maand na beëindiging door te zetten. Opdrachtgever en opdrachtnemer hebben na beëindiging van de ondernemer verder geen financiële verplichtingen meer naar elkaar.

5.5 Opzegging

Bij opzegging van de dienst door opdrachtgever, zal opdrachtnemer binnen 1 maand na het stopzetten van de licentie alle gebruikersdata vernietigen.

5.6 Ondersteuning en helpdesk

Ondersteuning voor medewerkers van opdrachtgever is op inhoud voor rekening van Opdrachtgever. Ondersteuning voor medewerkers van opdrachtgever bij technische fouten is voor rekening van opdrachtnemer. Voorbeeld: een medewerker die een wachtwoord vergeten is of een activatiemail in zijn/haar spamfilter heeft zien verdwijnen wordt geholpen door opdrachtgever. Wanneer de automatisch gegenereerde e-mail vanuit de optie ‘wachtwoord vergeten’ niet werkt, zal dit verholpen worden door opdrachtnemer.
Primair aanspreekpunt voor alle medewerkers over gebruik van het platform ligt bij Opdrachtgever. Wanneer Opdrachtgever vermoedt dat er sprake is van een technische fout, kan per e-mail contact gezocht worden met opdrachtnemer.
Opdrachtnemer zal binnen 24 uur naar opdrachtgever reageren op technische fouten en deze binnen 5 werkdagen verhelpen of een verwachte tijdsplanning delen voor het verhelpen van de technische fouten.
Opdrachtnemer houdt contact met één of een klein aantal aanspreekpunt(en) van opdrachtgever en communiceert niet direct met overige medewerkers van opdrachtgever.

5.7 Problem and Incident Management

In het geval een incident zal deze zo snel mogelijk volgens de richtlijnen uit artikel 6 van het voorstel worden voorzien van een hotfix en kan direct naar de productieomgeving worden gezet.

5.8 Change Management

Elke wijziging op het systeem wordt opgenomen in versiebeheer (GIT). Na elke wijziging worden alle testcases automatisch gerund. Enkel wanneer alle tests slagen, wordt de wijziging naar de acceptieomgeving gelanceerd. Daar worden nog eventueel handmatige tests uitgevoerd door opdrachtnemer. Bij akkoord kan met een druk op de knop de exacte software op de acceptatieomgeving verplaatst worden naar de productieomgeving. Mochten er onverhoopt toch fouten voordoen in de productieomgeving is het een druk op de knop om de vorige versie terug te zetten.

5.9 Capacity Management

De servers waar de software op draait, worden continu en automatisch gemonitord. Voordat capaciteitsproblemen zich voordoen, triggert deze software alerts naar de staf van Welder. Als blijkt dat er een kans is op een gebrek aan capaciteit, zal er tijdig capaciteit worden toegevoegd.

5.10 Availability Management

Verschillende uptime monitors controleren continu de beschikbaarheid van verschillende componenten. Zodra deze niet beschikbaar zijn, wordt er automatisch een bericht verstuurd aan de staf van Welder. De ontvangers vanuit Welder nemen hierop passende maatregelen.

5.11 Continuity Management

Welder analyseert regelmatig of er sprake is van risico's die de continuïteit van de software in gevaar brengen en zal opdrachtgever hier tijdig over informeren. Dagelijks wordt een back-up gemaakt van het hele systeem. Periodiek worden deze back-ups getest, zodat we zeker weten dat deze back-ups werken.

5.12 Identity & Authorisation Management

Welder stelt alleen medewerkers van opdrachtgever in staat gebruik te maken van de software. Op welke wijze dit het meest efficiënt kan gebeuren, zal worden bepaald gedurende de opdracht.

5.13 Recovery Point Objective (RPO)

Van bestanden wordt elke nacht een back-up gemaakt, waarmee maximaal dataverlies een dag bedraagt. Van de database wordt continu (point-in-time recovery) gemaakt met offsite sync elke vijf minuten.

5.14 Recovery Time Objective

Wordt periodiek getest. Daadwerkelijke herstelperiode is binnen 24 uur.

5.15 Rapportagemogelijkheden

Het gebruik van het platform kan geanalyseerd worden. In dit voorstel zijn hiervan screenshots opgenomen.

5.16 Kwetsbaarheden managen / patchen

Elke nacht wordt er gecheckt op beschikbaarheid van nieuwe patches van het OS. Bij beschikbaarheid worden deze automatisch geïnstalleerd. De externe software componenten worden regelmatig gecheckt op security patches.

5.17 User accounts / wachtwoordbeleid

Iedere user heeft een account met wachtwoord. Wachtwoorden worden voorzien van een salt en met een one way hash (Bcrypt) opgeslagen. Single Sign On met systemen van opdrachtgever wordt nader afgestemd. In geval van Single Sign On is het opslaan van wachtwoorden wellicht overbodig.

5.18 Gebruikersrechten

Op technisch niveau: toegang tot server beperkt tot developers van Welder.
In CMS: vanuit opdrachtgever kunnen bepaalde personen admin-rechten krijgen en gebruikersrechten toekennen.

5.19 Security baselines / hardening

Welder gebruikt standaard security patches van het OS. Geen extra hardening.

5.20 Uitdiensttreding personeel Welder

Toegang tot server is middels SSH keys. bij uitdiensttreding wordt de public key van de medewerker in kwestie verwijderd.

5.21 Uitdiensttreding personeel opdrachtgever

Wanneer gebruikers uit dienst gaan (op basis van de gedefinieerde uitdienstdatum), wordt het account verwijderd en kan gebruiker niet meer inloggen.

5.22 Monitoring

Als de site offline gaat, worden berichten gegenereerd. Het is enkel mogelijk om vanaf whitelisted IP-adressen toegang te krijgen tot de server. Andere IP-adressen worden door de firewall geblokkeerd.

5.23 Anti malware en –virus

De software draait onder Linux, met actief patch management wordt het risico op virus of malware beperkt. Daarnaast draait alle software geïsoleerd in Docker containers. Dit zorgt ervoor dat alle processen volledig geïsoleerd zijn en gevolgen van malware of virussen beperkt blijven.

5.24 Ontsluiting naar eindgebruikers

Door de applicatie te downloaden via de App Store (iOS) of Play store (Android), danwel deze via een nader overeen te komen subdomein van welder.nl te benaderen in een webbrowser. Het gebruikelijke scenario verschilt per opdrachtgever.

5.25 Encrypted data

Alle data is encrypted, zowel ‘at rest’ als tijdens verzending. Tijdens verzending wordt data encrypted via https.

5.26 Opslag binnen EU

Hetzner datacenter in Falkenstein (Duitsland). Opslag/verwerking binnen EU wordt gegarandeerd. Hetzner is een ISO 27001 gecertificeerd datacenter.
Back-ups worden opgeslagen bij OVH in Frankrijk. OVH is ook ISO 27001 gecertificeerd

Hoofdstuk 6 | **Data Protection Impact Assessment (DPIA)**

Door:	Welder
Datum uitvoering:	maart 2025

Eens per twee jaar wordt een DPIA uitgevoerd om te kijken of de huidige maatregelen nog voldoende zijn. Wanneer er structurele zaken veranderen, bijvoorbeeld wanneer er een significante wijziging is aantal/type persoonsgegevens dat verwerkt wordt of de samenwerking met subverwerkers verandert, kan ervoor gekozen deze DPIA vaker uit te voeren. Deze wordt dan intern uitgevoerd door de privacy officer van Welder, eventueel onder advies / begeleiding van een externe adviseur. De hoofdstukken 1 tot en met 6 die hierna genoemd worden gelden als voornaamste hoofdstukken bij het uitvoeren van deze DPIA.

6.1 De Verantwoordelijke

Welder is in overeenkomsten met Opdrachtgevers de Verwerker en de Opdrachtgever is de verwerkingsverantwoordelijke.

6.2 De Verwerking van de persoonsgegevens en rechtmatigheid

Categorie persoonsgegevens:	persoonsgegevens van klanten, leveranciers, medewerkers en andere relaties
Categorie betrokkenen:	werknemers
Grondslag voor verwerking:	wettelijke grondslag 1: Verwerker heeft toestemming van de betrokkene om de gegevens te verwerken. Elke betrokkene wordt uitdrukkelijk om toestemming gevraagd voordat gebruik gemaakt wordt van de systemen van Verwerker.
Doel van de verwerking:	Verwerker zal Persoonsgegevens verwerken, waarvoor Verwerkingsverantwoordelijke verantwoordelijk voor is, omdat hiermee enerzijds de betrokkene beter geholpen kan worden met de persoonlijke ontwikkeling en anderzijds de Verwerkingsverantwoordelijke inzichten genereert die de strategische personeelsplanning verbeteren.
Locatie verwerker:	’s-Hertogenbosch, Nederland.
Bewaartermijn:	De data wordt opgeslagen zonder einddatum. Met elke Opdrachtgever maakt Welder afspraken over het al dan niet verwijderen van data na een bepaalde periode. Zonder expliciet verzoek van Opdrachtgever is dat zonder einddatum. Wanneer een medewerker (betrokkene) van een Opdrachtgever (verwerkingsverantwoordelijke) vraagt om het verwijderen van de persoonlijke data, zal dat altijd gehonoreerd worden.
Veiligheidsmaatregelen:	Zie hoofdstukken 2 en 4

6.3 Manier van verwerking

Welder verzamelt de persoonsgegevens op een drietal manieren.

a) In sommige gevallen wordt er een **automatische koppeling** gelegd met een personeelsregistratiesysteem van een Opdrachtgever. In dat geval worden persoonsgegevens zoals indienstdatum of geboortedatum automatisch overgenomen uit het salarispakket van Opdrachtgever en geregistreerd in het platform van Welder.

b) Daarnaast kan het zijn dat een medewerker **zelf informatie ingeeft**. Een medewerker geeft bijvoorbeeld informatie over zijn of haar hobby's of upload een profielfoto of telefoonnummer. Deze informatie wordt door Welder opgeslagen.

c) Tenslotte worden bepaalde handelingen van medewerkers **onderhuids geregistreerd**. Denk bijvoorbeeld aan informatie over wanneer mensen hebben ingelogd of welke pagina's zij bezocht hebben. Deze informatie kan Welder helpen de software telkens te verbeteren en de opdrachtgever om inzichten te genereren.

6.4 Opslag van de persoonsgegevens

Welder zorgt ervoor dat gegevens opgeslagen worden in de databases van de hosting provider Hetzner te Duitsland. De inrichting van deze databases wordt vormgegeven door de ontwikkelaars van Welder en onafhankelijk getoetst door externe auditors.

6.5 Noodzakelijkheid van de verwerking

De verschillende persoonsgegevens hebben hun eigen noodzakelijkheid. Sommige persoonsgegevens worden verzameld vanuit een praktisch oogpunt. Zonder bijvoorbeeld een e-mailadres kunnen we een medewerker geen uitnodiging sturen voor een medewerkersonderzoek. Andere persoonsgegevens worden verzameld om de juiste inzichten te verzamelen voor een strategische personeelsplanning. Zo worden leidinggevenden gevraagd informatie te geven over het ingeschatte potentieel van medewerkers gebruikt voor automatische analyses door het management van de opdrachtgevers. Tenslotte worden persoonsgegevens verwerkt om de medewerker te helpen bij de persoonlijke ontwikkeling. Zo kan een medewerker tijdens de voorbereiding van een functioneringsgesprek inzicht geven in de persoonlijke werktevredenheid. Deze data moet verzameld en verwerkt worden, zodat leidinggevende en medewerker samen tijdens het gesprek een actieplan kunnen maken rond de persoonlijke ontwikkeling van medewerkers.

6.6 Evaluatie risico's bij de verwerking

Bij het evalueren van de risico's is sprake van twee belangrijke aspecten: 1) de kans dat data niet goed verwerkt wordt en 2) de impact van wat er kan gebeuren als deze data niet goed verwerkt wordt.

De kans dat data niet goed verwerkt wordt, acht Welder relatief laag. Dit omdat er veel technische maatregelen zijn genomen (hoofdstuk 2) en omdat deze maatregelen onafhankelijk getoetst worden door een extern bureau (hoofdstuk 4).
Het is goed om te realiseren wat er gebeurt wanneer onverhoopt de data niet goed verwerkt wordt. Het meest waarschijnlijke scenario is dat een proces doorbroken wordt richting een medewerkers. Een medewerker ontvangt bijvoorbeeld een e-mail niet. Of informatie is verloren gegaan en moet opnieuw ingegeven worden. De impact

is dan relatief laag en vaak maar van toepassing op één medewerker. In een onwaarschijnlijker scenario wordt data beschikbaar voor derden. Personeelsgegevens komen bijvoorbeeld in handen van hackers of commerciële instellingen. In een impact-schaal van laag-midden-hoog, schatten we de impact dan op 'midden'. Enerzijds komen veel gegevens dan 'op straat' te liggen. Anderzijds classificeren we de verwerkte data niet als hoog privacygevoelig. De persoonsgegevens die Welder verwerkt zijn bijvoorbeeld minder privacygevoelig dan bijvoorbeeld bankrekeninggegevens of medische gegevens.

6.7 Beschrijving voorgenomen maatregelen

Alle medewerkers van Welder worden tijdens het inwerkprogramma gewezen op alle genomen veiligheids- en privacymaatregelen. Daarnaast worden in vast periodiek overleg alle nieuwe ontwikkelingen besproken. En het is een vast onderdeel in de jaarplannen van Welder. Daarnaast zal de periodieke externe toets blijven plaatsvinden om eventuele 'blinde vlekken' eruit te halen.

Hoofdstuk 7 | **Penetratie testen**

Jaarlijks laat Welder een penetratietest uitvoeren door een onafhankelijk, extern beveiligingsbedrijf om de veiligheid van onze software te waarborgen. Deze tests simuleren aanvallen van kwaadwillenden om kwetsbaarheden te identificeren en op te lossen.

De managementrapportages van de meest recente penetratietesten zijn beschikbaar op onze website (https://www.welder.nl/trust-center). Daarnaast is het, in overleg, mogelijk om een extra penetratietest uit te laten voeren. Welder verleent onder enkele voorwaarden hier volledige medewerkers toe. Neem contact op via security@welder.nl om dit verder te bespreken.

Hoofdstuk 8 | **Externe toets door De Functionaris**

Naast een technische toets op de functionele veiligheidsmaatregelen, laat Welder haar beleid periodiek extern toetsen op het gebied van privacy- en beleidsmaatregelen. De laatste audit is uitgevoerd in juli 2023 door het bureau De Functionaris uit Capelle a/d Ijssel (KvK 6915829). Dit bureau is gespecialiseerd in privacywetgeving (AVG). Door deze twee externe toetsen periodiek uit te laten voeren, borgt Welder dat de juiste maatregelen genomen zijn om de veiligheid van data van (medewerkers van) opdrachtgevers te waarborgen.

De resultaten van de audit zijn telkens openbaar. Hierna volgen de resultaten van de laatste toets.

DE FUNCTIONARIS
JURIDISCHE DIENSTVERLENING

Audit AVG-compliance en de controle van juridische documenten

Opdrachtgever	:	WELDER B.V.
Verzorgd door	:	L.A. van der Leeden DE FUNCTIONARIS B.V.
Datum	:	7 juli 2023

1

DE FUNCTIONARIS
JURIDISCHE DIENSTVERLENING

Inhoudsopgave

1. Achtergrond 3
2. AVG-compliance 3
3. Controle van de juridische documenten 4
4. Werkwijze en audit 5
5. Achtergrond 15
6. Overzicht van potentiële risico's 15
7. Risico-inventarisatie 15
8. Conclusie audit en risico-inventarisatie 17

DE FUNCTIONARIS
JURIDISCHE DIENSTVERLENING

1. Achtergrond

Alle bedrijven en instellingen in de Europese Unie moeten voldoen aan de Algemene Verordening Gegevensbescherming (hierna: de AVG). Het naleven van deze wetgeving vraagt de nodige technische en organisatorische maatregelen en vereist structurele aandacht om AVG-compliant te blijven.

WELDER heeft aangegeven kritisch te willen kijken naar haar eigen (bedrijfs)processen en de al bestaande maatregelen op het gebied van gegevensbescherming en informatiebeveiliging. Ook wil WELDER de door haar gebruikte standaardovereenkomsten en offertes op (juridische) juistheid controleren.

WELDER heeft hiervoor De Functionaris ingeschakeld om een audit uit te voeren. De audit wordt uitgevoerd aan de hand van een (digitale) bespreking met WELDER en de nader toegestuurde documenten en beleidsstukken. De Functionaris zal de audit uiteindelijk in een Plan van Aanpak omzetten, zodat duidelijk is welke stappen WELDER nog zal moeten zetten om volledig AVG-compliant en haar standaardovereenkomsten en offertes te laten voldoen aan de daarvoor geldende wettelijke vereisten.

Mocht WELDER deze openstaande werkzaamheden willen laten oppakken (en onderhouden) door De Functionaris, dan is dit uiteraard mogelijk. Na het onderdeel “audit” doet De Functionaris daarom in dit document een vrijblijvend voorstel om deze werkzaamheden uit te voeren. Op basis van de bevindingen, de tevredenheid over de uitvoering van de werkzaamheden en de bereidheid van WELDER kan na de uitvoering van het Plan van Aanpak een Functionaris voor Gegevensbescherming (FG) worden aangesteld. Hiervoor stelt De Functionaris tegen die tijd een passend voorstel op voor de externe aanstelling daarvan.

2. AVG-compliance

De AVG vereist dat een organisatie verwerkingen van persoonsgegevens in kaart brengt, daarover (op verzoek) verantwoording aflegt en klanten/leveranciers daarover op een begrijpelijke wijze kan informeren. Concreet komt dit neer op de volgende verplichtingen:

1. Het voldoen aan de AVG documentatieplicht door middel van een gedegen en toekomstbestendig privacy beleid, waaronder:
    - Het in kaart brengen van alle verwerkingen door middel van een verwerkingsregister (art. 30 AVG);
    - Het in kaart brengen van (sub)verwerkers en het overeenkomen van de noodzakelijke verwerkersovereenkomsten.

- Het in kaart brengen van de huidige privacy risico's en documenteren van rechtmatigheid/doelbinding bij huidige verwerkingen;
- Het doen van aanbevelingen ten aanzien van gebruikte gegevensverwerkingsinstrumenten, met het oog op de in wetgeving vereiste concepten als dataminimalisatie, dataportabiliteit, etc.

2. Het voldoen aan de AVG verantwoordingsplicht, waaronder;
   - Handboek Privacybeleid (art. 24 AVG);
   - Bijdragen aan privacy-bewustwording op de werkvloer door middel van presentaties/trainingen (art. 39 AVG);
   - Structureel inplannen van evaluatiemomenten (art. 32 AVG);
   - Onderzoeken verplichting aanstellen Functionaris voor de Gegevensbescherming (art. 37 AVG);
3. Het voldoen aan de AVG informatieplicht, waaronder
   - Transparantie van informatie en communicatie, zowel intern als extern (art. 12 AVG);
   - Waarborging van de rechten van betrokkenen (art. 15-22 AVG), denk aan inzage, correctie, dataportabiliteit, verwijdering etc.;
   - Instellen procedure 'Meldplicht datalekken' (art. 33-34 AVG);
4. Overige verplichtingen/bepalingen;
   - Onderzoeken mogelijkheid aansluit bij certificering (art. 42 AVG);
   - Website(s) inhoud t.a.v. aansprakelijkheid, cookies, gegevensverwerking en de wettelijke informatieverplichtingen.

3. Controle van de juridische documenten

WELDER heeft in het kader van deze audit meerdere (standaard)overeenkomsten en documenten aangeleverd die zij gecontroleerd willen zien. Het gaat, meer specifiek, om de volgende stukken:

1. Offerte,
   - De algemene voorwaarden;
   - Implementatiestappen WELDER;
   - Beveiligings- en privacybeleid;
   - Aanpassingskader;
   - DEV-roadmap.
2. De (standaard)verwerkersovereenkomst;
3. Privacy Statement;
4. De (standaard)arbeidsovereenkomst;
5. Polisbladen ASR en Verhoeven Verzekeringen.

DE FUNCTIONARIS
JURIDISCHE DIENSTVERLENING

4. Werkwijze en audit

Op basis van 'AVG-Compliance' en 'Controle van de juridische documenten' zal een uiteenzetting worden gemaakt van hoe WELDER dit op dit moment heeft ingeregeld en welk resultaat gewenst is. Deze resultaten staan hieronder genoemd met daarbij een voorgesteld middel om dat resultaat te bereiken.

De audit is zichtbaar in onderstaand schema. Het schema is ingevuld aan de hand van de door WELDER aangeleverde documentatie en hetgeen er tijdens de (digitale) meetings met Leonard van der Leeden is besproken.

Om het overzicht te houden hebben wij aan de hand van de beoordeling de resultaten als volgt weergegeven:

- Groen (volledig door WELDER opgepakt);
- Oranje (gedeeltelijk door WELDER opgepakt) of,
- Rood (niet door WELDER opgepakt).

DE FUNCTIONARIS
JURIDISCHE DIENSTVERLENING

	Resultaat	Beoordeling	Voorgesteld middel
1.	**AVG-documentatieplichten | Grondslag en rechtmatige verwerking**		
1.1	Leg een register van verwerkingen aan (art. 30 AVG)	Een verwerkingsverantwoordelijke is gehouden om een register van verwerkingsactiviteiten aan te leggen (art. 30.1 AVG). Hierin moet het volgende worden opgenomen: • Naam en contactgegevens van de organisatie; • De verwerkingsdoelen • Omschrijving van de categorieën van betrokkenen en de persoonsgegevens; • Categorieën van ontvangers aan wie de persoonsgegevens zijn verstrekt; • Eventuele doorgiften aan een derde landen (buiten de EER); • Bewaartermijnen; • Een algemene beschrijving van de genomen beveiligingsmaatregelen. In hoofdstuk 4 van het Beveiligings- en privacybeleid van WELDER heeft zij de gegevensverwerking beschreven ten aanzien van de terbeschikkingstelling van de software aan eindgebruikers. Deze omschrijving omvat het verwerkingsdoel, benoemt de categorieën van betrokkenen en de gegevens, de doorgifte van gegevens aan het buitenland (de Duitse hostingpartner). Een algemene beschrijving van de bewaartermijnen wordt gemist, maar is wel in de eveneens in het document opgenomen DPIA benoemd (p. 16). Hetzelfde geldt voor de genomen beveiligingsmaatregelen. Het verdient de voorkeur om deze ook bij de omschrijving van de gegevensverwerking te benoemen.	

6

1.1.1	Bepaal wie in welke gevallen verwerkingsverantwoordelijke en wie de verwerker is	Zie beoordeling onder 1.1	
1.1.2	Breng alle verwerkingen van persoonsgegevens binnen WELDER in kaart	Het door WELDER aangedragen Beveiligings- en privacybeleid is specifiek gericht op de gegevensverwerking die samenhangt met het ter beschikking stellen van de software aan klanten. Hoewel dat op zichzelf niet onjuist is, vereist de AVG dat WELDER alle gegevensverwerkingen binnen de organisatie in kaart brengt en beschrijft. Daarbij kan worden gedacht aan: • Salarisadministratie; • Financiële administratie; • Personeelszaken; • Websitebeheer; • Verzekeraars/pensioenvoorziening. Dergelijke gegevensverwerkingen heeft WELDER niet (in de aangeleverde stukken) beschreven. Het verdient aanbeveling dat deze verwerkingen, los van de verwerkingen die WELDER aan de klant ter beschikking stelt, worden uitgewerkt.	
1.1.3	Waarborg dat verwerkers een register bijhouden met contactgegevens;	Ontbreekt momenteel	
1.1.4	Toetsing van verwerking van persoonsgegevens op rechtmatigheid (art. 5, 6 en 9 AVG)	De beschreven gegevensverwerking is in hoofdstuk 4 het Beveiligings- en privacybeleid van WELDER getoetst op rechtmatigheid, waarbij eveneens de relevante grondslagen zijn benoemd. De bepalingen uit artikel 9 van de AVG	

7

		zijn niet op de gegevensverwerking van toepassing. Voor het overige wordt verwezen naar de beoordeling onder 1.1.2.	
1.2	De organisatie weet wanneer er toestemming voor een gegevensverwerking kan worden gevraagd en kan dit vastleggen (art. 6 en 7 AVG)	Onder toestemming wordt volgens de AVG het volgende verstaan (zie 4.11 AVG): Een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting, waarmee de betrokkene door middel van een verklaring of actieve handeling de verwerking van persoonsgegevens accepteert. In het Beveiligings- en privacybeleid van WELDER is beschreven dat de gegevensverwerking (gedeeltelijk) is gebaseerd op toestemming. Hierin staat onder andere dat de gebruiker alleen van de software gebruik kan maken, wanneer deze toestemming geeft. Uit de overwegingen uit de AVG kan worden opgemaakt dat er geen sprake is van vrijelijk gegeven toestemming als de uitvoering van de overeenkomst, daaronder begrepen het verlenen van diensten, afhankelijk wordt gesteld van toestemming van de betrokkene, terwijl die toestemming niet nodig is voor het verlenen van de dienst. Op basis van welke informatie is WELDER overgegaan tot het gebruik van toestemming als verwerkingsgrondslag? Het nadeel daarvan is namelijk dat er toestemming in een arbeidsrelatie niet snel vrijelijk kan worden verkregen, vanwege de gezagsverhouding tussen werknemer en werkgever. Wij menen dat de grondslag gerechtvaardigd belang beter op deze situatie aansluit. Het is wel noodzakelijk dat dit belang goed in het beleid wordt omschreven.	

8

1.3	Review en actualiseer huidige verwerkersovereenkomsten	Het gaat hier om verwerkersovereenkomsten die WELDER met haar toeleveranciers heeft afgesloten. Er is vanuit de organisatie aangegeven dat er bepaalde verwerkersovereenkomsten zijn afgesloten. Het is echter onduidelijk in hoeverre deze zijn gecontroleerd door iemand met het vereiste kennisniveau. Ook zullen er hoogstwaarschijnlijk meer partijen aanwezig zijn waarmee WELDER alsnog een verwerkersovereenkomst moet afsluiten.	
1.4	Documenteer een volledig beleid, de processen, procedures taken en maatregelen om aan te tonen dat aan de AVG wordt voldaan.	Op dit moment is het primaire proces/procedure gedeeltelijk door WELDER beschreven in de DPIA die het beveiligings- en privacybeleid is opgenomen. De overige processen zijn hierin niet beschreven. Voor het overige wordt verwezen naar de beoordeling onder 1.1.2	
2.	**AVG-documentatieplichten | Grondslag en rechtmatige verwerking**		
2.1	Analyseer en beschrijf de huidige technische maatregelen	In het beveiligings- en privacybeleid heeft WELDER een lijst met technische maatregelen beschreven. Deze lijst is omvangrijk, maar het is niet vast te stellen of deze daadwerkelijk een volledige opsomming biedt.	
2.2	Leg de principes 'privacy by design'/'privacy by default' vast in een beleid van de organisatie.	In hoofdstuk 5 van het beveiligings- en privacybeleid van WELDER is ingegaan op de beginselen van Privacy by Design en Privacy by Default (p. 12). De development afdeling wordt getraind in deze uitgangspunten en bij verdere ontwikkelingen worden deze beginselen als uitgangspunt gehanteerd.	
2.3	Richt een proces in om te kijken of een DPIA nodig is en om een DPIA uit te voeren (inclusief model DPIA).	Uit het beveiligings- en privacybeleid blijkt dat WELDER in mei 2022 een DPIA heeft uitgevoerd. De achterliggende reden/noodzaak voor het uitvoeren van de DPIA is daaruit echter niet op te maken en bovendien is niet gebleken dat deze heeft plaatsgevonden op basis van het in het beveiligings- en	

9

		privacybeleid beschreven proces. Geadviseerd wordt om dit in het privacybeleid te beschrijven.	
2.4	Wachtwoordbeleid	In hoofdstuk 5 van het beveiligings- en privacybeleid van WELDER (p. 14) is het wachtwoordbeleid op hoofdlijnen beschreven.	
2.5	Autorisatiemodel (toelichting/theorie) en autorisatiematrix	In hoofdstuk 3 van het beveiligings- en privacybeleid van WELDER is in alinea 3.2 het autorisatiemodel/matrix opgenomen.	
3.	**AVG-documentatieplichten | Data Governance**		
3.1	Wijs binnen de organisatie rollen en verantwoordelijkheden expliciet aan	In hoofdstuk 3 van het beveiligings- en privacybeleid van WELDER is in alinea 3.4 de rolverdeling genoemd.	
3.2	Train verantwoordelijken en personeel over de verplichtingen uit de AVG	Alle medewerkers van WELDER ontvangen bij indiensttreding een digitale training op het gebied van gegevensbescherming. Daarna ontvangt elke medewerker 1x per jaar een training op het gebied van gegevensbescherming. De inhoud hiervan wordt opgesteld door de privacy officer.	
3.3	Maak voldoende budget vrij voor het privacy programma	WELDER heeft aangegeven maatregelen te nemen op het gebied van gegevensbescherming om zo volledig AVG compliant te worden.	
3.4	Zorg voor een periodieke evaluatie van maatregelen	In hoofdstuk 3 van het beveiligings- en privacybeleid van WELDER is in alinea 3.10 aangegeven dat de beleidsmaatregelen eenmaal per jaar met de FG en directie worden geëvalueerd en geüpdatet.	
3.5	Sluit mogelijk aan bij een gedragscode of certificeren (art. 24.3 AVG)	Nog geen onderzoek naar het aansluiten bij een gedragscode of certificering verricht.	

3.6	Functionaris voor Gegevensbescherming	In hoofdstuk 3 van het beveiligings- en privacybeleid van WELDER is in alinea 3.4 aangegeven dat Ferry van Hooydonk is aanwezen als Privacy Officer/Functionaris Gegevensbescherming. Een FG is een interne privacy-toezichthouder. Dit toezicht moet op onafhankelijke wijze plaatsvinden. De AP heeft in het verleden zorgen geuit over de combinatie van de rol van PO en FG. De medewerker die het privacybeleid mede-vormgeeft, zou daarmee namelijk dezelfde persoon zijn die dat beleid vervolgens als onafhankelijk toezichthouder moet controleren. Het combineren van deze twee functies kan volgens de AP tot mogelijke belangenconflicten leiden, met mogelijke risico's voor de privacy van betrokkenen. Geadviseerd wordt dan ook om beide rollen (PO enerzijds, FG anderzijds) van elkaar te scheiden.	
4.	**AVG-documentatieplichten | Transparantie van informatie en communicatie**		
4.1	Tref 'passende maatregelen' om te communiceren met betrokkenen	In de arbeidsovereenkomst zijn de nodige aanpassingen doorgevoerd. De vraag is wel hoe WELDER dit heeft geregeld in reeds afgesloten overeenkomsten?	
4.1.1	Medewerkers – Regelement Privacy	Dit is opgenomen in de arbeidsovereenkomst. Zie hiervoor eveneens de toelichting onder 4.1.	
4.1.2	Medewerkers – Regelement ICT-gebruik en Sociale Media	Dit is opgenomen in de arbeidsovereenkomst. Zie hiervoor eveneens de toelichting onder 4.1.	
4.1.3	Medewerkers – formulier toestemming voor het publiceren van beeldmateriaal	Dit is opgenomen in de arbeidsovereenkomst.	

11

4.1.4	Medewerkers – procedure voor uitdiensttreding van medewerkers	Beschreven in artikel 5.20 van het Beveiligings- en privacybeleid van WELDER.	
4.2	Rechten van betrokkenen (art. 15 tot 22 AVG)	Beschreven in de arbeidsovereenkomst voor medewerkers. Zie hiervoor eveneens de toelichting onder 4.1.	
4.2.1	Inzage (art. 15 AVG)		
4.2.2	Rectificatie (art. 16 AVG)		
4.2.3	Wissing (art. 17 AVG)		
4.2.4	Beperking van de verwerking (art. 18 AVG)		
4.2.5	Kennisgeving (art. 19 AVG)		
4.2.6	Dataportabiliteit (art. 20 AVG)		
4.2.7	Bezwaar (art. 21 AVG)		
4.2.8	Vragen en klachtenprocedure		
4.3	Meldplicht datalekken (art. 33-34 AVG)		
5.	**Website**		
5.1	Cookies	Op welder.nl is een cookiemelding geplaatst, maar deze voldoet niet. Tracking cookies worden geplaatst, ongeacht of er wel/geen toestemming wordt gegeven. Ook is er geen mogelijkheid tot afwijzen van de cookies. Daarnaast is er een cookieverklaring op de website aanwezig, maar ook deze voldoet niet. Een overzicht waar de geplaatste cookies worden opgesomd, inclusief functie en bewaartermijn, ontbreekt momenteel.	Oplossing CookieCode en beschrijving in privacybeleid

12

5.2	Privacyverklaring	Er is een privacyverklaring aanwezig op welder.nl, hierin wordt aangegeven welke persoonsgegevens er worden verwerkt en voor welke doeleinden.	Oplossing CookieCode en beschrijving in privacybeleid
5.3	Beveiligde verbinding	Op welder.nl is gebruik gemaakt van een beveiligde verbinding.	SSL-certificaat op de website waar de gegevensverwerking plaatsvindt.
6.	**Controle van de aangeleverde juridische documenten**		
6.1	De standaardofferte	De standaardofferte voldoet aan de gestelde vereisten.	
6.2	De verwerkersovereenkomst	De verwerkersovereenkomst van WELDER is op hoofdlijnen gecontroleerd. Hieruit is gebleken dat er geen afwijkende of ongebruikelijke bepalingen in deze overeenkomst zijn opgenomen. Verdere aanpassingen van de verwerkersovereenkomst zijn niet noodzakelijk.	
6.3	De algemene voorwaarden	De algemene voorwaarden van WELDER zijn op hoofdlijnen gecontroleerd. Hieruit is gebleken dat er geen afwijkende of ongebruikelijke bepalingen in deze algemene voorwaarden zijn opgenomen. Verdere aanpassingen van de algemene voorwaarden zijn niet noodzakelijk.	
6.4	De arbeidsovereenkomst	De arbeidsovereenkomst van WELDER is op hoofdlijnen gecontroleerd. Hieruit is gebleken dat er geen afwijkende of ongebruikelijke bepalingen in deze arbeidsovereenkomst zijn opgenomen. Verdere aanpassingen van de arbeidsovereenkomst zijn niet noodzakelijk. Wel is WELDER verplicht het Privacy- en Beveiligingsbeleid, waarnaar in artikel 13 wordt verwezen, overgelegd wordt met de overeenkomst.	
6.5	Verzekeringen / Polisbladen	WELDER heeft via ASR een werkgeversaansprakelijkheidsverzekering afgesloten. Deze is gebaseerd op een jaaromzet van 1.3 miljoen. WELDER dient na te gaan in hoeverre de ingeschatte jaaromzet overeenkomt met de daadwerkelijke jaaromzet. Indien hier grote verschillen zouden bestaan, dient	Op het eerste gezicht lijkt de verzekering voor de aansprakelijkheid de dienstverlening van WELDER

13

		met ASR in contact te worden getreden over een aanpassing van deze omzet, omdat dit uiteindelijk ook zijn weerslag heeft op het verzekerde bedrag. De verzekerde activiteit is het voeren van een organisatieadviesbureau. Vervolgens moet worden vastgesteld dat ASR in haar verzekeringsvoorwaarden een uitzondering voor deze verzekering heeft bedongen, wanneer de schade het gevolg is van het niet, niet op tijd, of niet goed leveren van de dienstverlening. Deze uitsluiting moet worden beoordeeld, eventueel in overleg de verzekeraar. Is het niet juist het uitvoeren van de dienstverlening waarvoor WELDER graag een verzekering als vangnet heeft bij aansprakelijkheid? Daarnaast heeft WELDER via Verhoeven Verzekeringen een 'WEGAS XL-verzekering' afgesloten (werk-gerelateerd verkeer). De verrichte controle heeft geen nadere aanbevelingen opgeleverd. Deze verzekering gaat uit van 12 medewerkers. Het is aan WELDER om te verifiëren of dit juist is. Op dit moment heeft WELDER geen verzekering voor risico's op het gebied van cyber crime of andere data gerelateerde risico's.	geheel uit te sluiten. Onderzoek nader of deze verzekering wel past bij het risico wat afgedekt dient te worden. Het is aan WELDER om uiteindelijk te beoordelen of de huidige dekking wenselijk is. Is het aantal werknemers nog conform de dekking in de WEGAS XL-verzekering? Gezien de (SaaS) dienstverlening en de aard van de werkzaamheden van WELDER strekt het aanbeveling een cyberverzekering te onderzoeken om aansprakelijkheid voor schade op dit specifieke gebied af te dekken.

14

5. Achtergrond

De Functionaris heeft op verzoek van WELDER een risico-inventarisatie uitgevoerd. Een risico-inventarisatie is een hulpmiddel om de potentiële risico's van een organisatie in kaart te brengen en deze (proactief) te beheersen. Ook kan op basis van deze risico-inventarisatie door WELDER worden bepaald welke conclusies en aanbevelingen als eerste worden opgepakt.

6. Overzicht van potentiële risico's

Bij het uitvoeren van de risico-inventarisatie wordt uitgegaan van de volgende risico's:

- Technische risico's, zoals storingen in apparatuur of software, systeemfouten of verminderde betrouwbaarheid van technologie.
- Gezondheids- en veiligheidsrisico's, zoals ongevallen op de werkvloer, gezondheidsproblemen en onveilige werkmethoden.
- Financiële risico's, zoals budgetoverschrijdingen, verlies van investeringen, gebrek aan financiering of veranderingen in de markt.
- Menselijke risico's, zoals onervarenheid van medewerkers, persoonlijke conflicten of wangedrag, en tekort aan gekwalificeerd personeel.
- Juridische risico's, zoals schendingen van wet- en regelgeving, inbreuk op intellectuele eigendomsrechten, of claims van derden.
- Operationele risico's, zoals vertragingen in leveringen, slechte planning of beperkingen in de productiecapaciteit.
- Reputatierisico's, zoals negatieve publiciteit, imagoschade of verlies van klantenvertrouwen.
- Strategische risico's, zoals veranderingen in de markt, concurrentie, of het niet voldoen aan verwachtingen van belanghebbenden.
- Risico's van externe factoren, zoals natuurrampen, politieke instabiliteit, of epidemieën.

7. Risico-inventarisatie

1. AVG-compliance
Risico's De AVG bepaalt dat de maximale boete die kan worden opgelegd 4% van de wereldwijde jaaromzet of 20 miljoen euro is, afhankelijk van welk bedrag hoger is. Non-compliance kan om die reden een grote invloed hebben op organisaties die met toezicht en handhaving worden geconfronteerd. De Autoriteit Persoonsgegevens (AP) is de toezichthouder op de privacywetgeving in

DE FUNCTIONARIS
JURIDISCHE DIENSTVERLENING

Nederland en heeft de bevoegdheid om handhavend op te treden tegen organisaties die niet voldoen aan de AVG. Dit kan leiden tot een formele waarschuwing, boete of het stilleggen van gegevensverwerkingen.

Daarnaast kan non-compliance leiden tot reputatieschade. Klanten en andere belanghebbenden kunnen het vertrouwen in de organisatie verliezen als gevolg van een datalek of overtreding van de AVG. Dit kan klanten aanleiding geven hun zaken elders te doen. Dit heeft weer verlies van omzet en marktaandeel tot gevolg.

Waarschijnlijkheid

In zijn algemeenheid mag gesteld worden dat de waarschijnlijkheid van overtreding van de AVG als vrij hoog kan worden aangemerkt, omdat het wetgeving met een brede reikwijdte betreft en het op vrijwel elke organisatie van toepassing is.

Daarbij moet de kanttekening geplaatst worden dat de toezichthouder over te weinig middelen beschikt de AVG op effectieve wijze te handhaven. Wel is de AP in beginsel verplicht om op basis van een klacht of handhavingsverzoek van een klant of andere betrokkene actie te ondernemen tegen overtredingen.

Beperking risico's:

Om de risico's te beperken, is het belangrijk dat WELDER haar privacybeleid en procedures voor datalekken op orde heeft. Ook het inbedden van gegevensbescherming op de werkvloer door meenemen/trainen van personeel is belangrijk, naast het duidelijk communiceren over dit onderwerp via bijvoorbeeld een personeelsbeleid.

2. Overige geconstateerde risico's

Risico's

Arbeidsovereenkomst: In de arbeidsovereenkomst ontbreekt een bepaling over het bestaan van een personeelsbeleid / handboek. Het niet hebben van een adequaat personeelsbeleid (o.a. voor privacy en gegevensbescherming) kan verschillende risico's met zich meebrengen. Zo kan er bijvoorbeeld onduidelijkheid bestaan over werktijden, procedure voor ziekmelding, de privacyrechten van medewerkers, kunnen persoonsgegevens van klanten onjuist verwerkt worden, of het gebruik van bedrijfsmiddelen.

Dit kan zich vertalen in juridische en financiële risico's t.o.v. het personeel en of derden waarmee personeel in aanraking komt.

Verzekeringen: Wanneer er geen verzekering is afgesloten, of wanneer deze niet dekkend is, dan kan dit grote financiële gevolgen hebben. De doorgegeven jaaromzet, aantal werknemers, of de verzekerde activiteit zijn hier bepalende factoren.
Waarschijnlijkheid: Arbeidsovereenkomst: Hoge mate van waarschijnlijkheid, veel bepalingen vanuit een personeelsbeleid komen dagelijks voor. Verzekeringen: Gemiddelde mate van waarschijnlijkheid, maar wel met grote gevolgen en risico's.
Beperking risico's: Arbeidsovereenkomst: Het is raadzaam om een adequaat personeelsbeleid op te stellen, en deze toe te voegen aan de huidige arbeidsovereenkomst. Verzekeringen: Onderzoek of er een cyberverzekering dient te worden afgesloten. Controleer daarnaast bij de huidig afgesloten verzekeringen of alle verstrekte gegevens en informatie kloppend zijn, zodat de verzekering ook daadwerkelijk dekkend is.

8. Conclusie audit en risico-inventarisatie

Uit de audit is gebleken dat WELDER stappen heeft gemaakt in het registreren van haar Privacy- en beveiligingsbeleid. Concreet dienen de volgende zaken als eerste te worden opgepakt:

- Het in kaart brengen van de gegevensstromen in een verwerkingsregister;
- De in deze de audit genoemde maatregelen op te pakken.

De Functionaris B.V.

L.A. (Leonard) van der Leeden

Reactie en plan van aanpak Welder
Per oranje (gedeeltelijk opgepakt) en rood (niet door Welder opgepakt) punt is een plan van aanpak opgesteld:

1.1.2 Breng alle verwerkingen van persoonsgegevens binnen Welder in kaart
De hoofdlijnen van gegevensverwerkingen zijn inmiddels beschreven in deze versie van het beveiligings- en privacybeleid. Hierbij dient opgemerkt te worden dat risico en impact bij klantgegevens als vele malen groter wordt ingeschat: Welder verzamelt persoonsgegevens van 100.000+ medewerkers en heeft zelf 'maar' ca 35 medewerkers in dienst.

1.1.3 Waarborg dat verwerkers een register bijhouden met contactgegegevens
Er is inmiddels een verwerkingsregister toegevoegd.

1.2 De organisatie weet wanneer er toestemming voor een gegevensverwerking kan worden gevraagd en kan dit vastleggen
Er is wat discussie over de grondslagen die gehanteerd worden. Deze hangen samen met de scope van het Welder platform. In artikel 4.8 is uitgebreid beschreven welke grondslagen van toepassingen (kunnen) zijn per module voor het verwerken van de bijbehorende persoonsgegevens. De opdrachtgever bepaalt welke grondslag het meest van toepassing is voor het gebruik van de software binnen de eigen organisatie.

1.3 Review en actualiseer huidige verwerkersovereenkomst
De verwerkersovereenkomst is geactualiseerd en opgenomen als addendum bij de algemene voorwaarden zodat die automatisch van kracht is op nieuwe overeenkomsten.

2.1 Analyseer en beschrijf de huidige technische maatregelen
Deze kunnen niet op volledigheid getoetst worden door De Funtionaris en daarom worden deze door andere externe bedrijven getoetst (zie hoofdstuk 7).

2.3 Richt een proces in om te kijken of een DPIA nodig is en om een DPIA uit te voeren
Dit is opgenomen in deze versie van het beveiligings- en privacybeleid.

3.5 Sluit mogelijk aan bij een gedragscode of certificeren
In 2025/2026 is het ISO27001 certificeringstraject gestart. Eind 2026 wordt het certificaat verwacht (zie hoofdstuk 11).

3.6 Functionaris voor gegevensbescherming
De rolverdeling van bepalen beleid en uitvoeren van beleid is gesplitst en opgenomen in dit beleid.

3.7 Medewerkers - formulier toestemming voor het publiceren van beeldmateriaal
Vanaf 2025 wordt dit als los document toegevoegd aan de arbeidsovereenkomst.

5.1 Cookies
Er is per direct een cookies-melding toegevoegd op Welder.nl

6.5 Verzekeringen / polisbladen

De werkgeversaansprakelijkheidsverzekering bij ASR is geactualiseerd op basis van huidige werknemersaantallen en omzet van Welder.

Hoofdstuk 9 | **Data Processing Addendum / Addendum Verwerkersovereenkomst**

Dit addendum vormt een aanvulling op de algemene voorwaarden van Welder (versie augustus 2026) en legt in het kader van de AVG de verplichtingen vast voor de verwerking van persoonsgegevens door de verwerker in opdracht van de verantwoordelijke.

1. Ten behoeve van de uitvoering van de Overeenkomst verstrekt Opdrachtgever aan Opdrachtnemer de opdracht tot Verwerking van Persoonsgegevens. Opdrachtgever en Opdrachtnemer zijn op basis van toepasselijke privacy wet- en regelgeving, in het bijzonder de AVG, verplicht een Verwerkersovereenkomst te sluiten. In het kader van deze Verwerkersovereenkomst is Opdrachtgever de “Verwerkingsverantwoordelijke” en Opdrachtnemer de “Verwerker”.
2. Verwerker Verwerkt Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke, op basis van diens schriftelijke instructies en onder diens verantwoordelijkheid en op de wijze vastgelegd in de Overeenkomst.
3. Verwerker Verwerkt de Persoonsgegevens slechts in opdracht van Verwerkingsverantwoordelijke, tenzij afwijkende wettelijke verplichtingen gelden.
4. Verwerker heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens en neemt geen beslissingen over het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens.
5. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk schriftelijk in kennis indien een instructie naar het redelijk oordeel van Verwerker inbreuk oplevert op de toepasselijke privacywetgeving.
6. Verwerker stelt op verzoek van Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de nakoming van in deze Verwerkersovereenkomst neergelegde verplichtingen aan te tonen.
7. Verwerker dient zorg te dragen voor de naleving van de voorwaarden die op grond van de toepasselijke privacywetgeving worden gesteld aan het Verwerken van Persoonsgegevens.
8. Verwerker verschaft enkel toegang tot de Persoonsgegevens aan haar werknemers voor zover dit nodig is voor het verrichten van de diensten op grond van de Overeenkomst. Verwerker waarborgt dat werknemers gebonden zijn aan een geheimhoudingsbeding.
9. Verwerker mag de Persoonsgegevens enkel buiten de EER Verwerken met voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke.
10. Verwerker zal alle passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen, garanderen een passend beveiligingsniveau gelet op de stand van de techniek, de uitvoeringskosten, alsook gelet op de aard, de omvang, context en verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's die Verwerking van de Persoonsgegevens die de Verwerker Verwerkt met zich meebrengen voor de rechten en vrijheden van de Betrokkenen. De geïmplementeerde beveiligingsmaatregelen zijn terug te vinden in het beveiligings- en privacybeleid (te vinden op de website).

11. Verwerker informeert Verwerkingsverantwoordelijke indien een van de beveiligingsmaatregelen wijzigt.
12. Verwerker staat toe dat Verwerkingsverantwoordelijke de naleving van de beveiligingsmaatregelen door Verwerker inspecteert of dat op verzoek van Verwerkeringsverantwoordelijke van gegevensverwerkingsfaciliteiten van Verwerker door een door Verwerkingsverantwoordelijk aan te wijzen onderzoeksinstantie worden geïnspecteerd in verband met de verwerkingsactiviteiten die onder deze verwerkersovereenkomst vallen. Verwerkingsverantwoordelijke draagt zorg dat de onderzoeksinstantie verplicht is tot geheimhouding van haar bevindingen tegenover derden.
13. Verwerkingsverantwoordelijke zal alle kosten, vergoedingen en onkosten in verband met de inspectie betalen, met inbegrip van redelijke door Verwerker gemaakte interne kosten.
14. Verwerkingsverantwoordelijke zal Verwerker een exemplaar van het rapport van de inspectie verstrekken.
15. Verwerker zal geen Persoonsgegevens aan een derde verstrekken of ter beschikking stellen tenzij op grond van een uitdrukkelijke schriftelijke opdracht van Verwerkingsverantwoordelijke of op bevel van een gerechtelijke of bestuurlijke instantie, op voorwaarde dat Verwerker in dat geval Verwerkingsverantwoordelijke zo spoedig mogelijk na ontvangst van een dergelijk bevel daarvan in kennis stelt om Verwerkingsverantwoordelijke zodoende in staat te stellen daartegen een haar ter beschikking staand rechtsmiddel in te stellen.
16. Verwerker zal Verwerkersverantwoordelijke schriftelijk om toestemming vragen om Persoonsgegevens aan derden te vertrekken en hiertoe pas overgaan na schriftelijke toestemming van Verwerkersverantwoordelijke.
17. Indien Verwerker van oordeel is dat zij op grond van een wettelijke verplichting Persoonsgegevens ter beschikking dient te stellen aan een daartoe bevoegde instantie zal zij daar niet toe overgaan, dan na overleg met en schriftelijke goedkeuring van Verwerkingsverantwoordelijke. Zij zal Verwerkingsverantwoordelijke zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die Verwerkingsverantwoordelijke redelijkerwijs nodig heeft om de benodigde maatregelen te treffen om te bepalen of verstrekking kan plaatsvinden en, zo ja, onder welke voorwaarden.
18. Verwerker dient Verwerkingsverantwoordelijke in kennis te stellen van alle verzoeken die rechtstreeks van Betrokkenen zijn ontvangen met betrekking tot de rechten van Betrokkenen op grond van de toepasselijke Privacywetgeving, waaronder maar niet beperkt tot verzoeken tot inzage, rectificatie, verwijdering, beperking van de verwerking of overdracht van de Persoonsgegevens. Verwerker geeft aan een dergelijk verzoek alleen gevolg indien Verwerkingsverantwoordelijke Verwerker daartoe schriftelijk opdracht heeft gegeven.
19. Verwerker handelt alle verzoeken om inlichtingen van Verwerkingsverantwoordelijke met betrekking tot de Verwerking van de Persoonsgegevens vlot en behoorlijk af conform de AVG.
20. Verwerker zal de Verwerkingsverantwoordelijke medewerking verlenen bij het doen nakomen van de verplichtingen om:
21. verzoeken van Betrokkenen met betrekking tot de uitoefening van rechten van Betrokkenen op grond van de toepasselijke Privacywetgeving te beantwoorden;

22. passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen;
23. datalekken te melden aan toezichthouder en de betrokkenen;
24. een Gegevensbeschermingseffectbeoordeling uit te voeren;
25. de toezichthouder te raadplegen voorafgaand aan een Verwerking de een hoog risico met zich meebrengt.
26. Verwerker mag een subverwerker inschakelen bij de uitvoering van deze Verwerkersovereenkomst. Indien een subverwerker wordt ingeschakeld om ten behoeve van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, zal Verwerker aan deze subverwerker bij overeenkomst minstens dezelfde verplichtingen inzake de Verwerking en bescherming van Persoonsgegevens opleggen als de verplichtingen die zijn opgenomen in deze Verwerkersovereenkomst. Voorafgaand aan het toevoegen/vervangen van een subverwerker, stelt Verwerker Verwerkingsverantwoordelijke hiervan schriftelijk in kennis, waarbij Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze verandering bezwaar te maken. Ten tijde van het aangaan van deze verwerkersovereenkomst is Verwerker gerechtigd om de Bijlage (beveiligings- en privacybeleid Welder) sub-verwerkers in te schakelen. Verwerker is in alle opzichten verantwoordelijk en aansprakelijk voor het doen en laten van derden die zij in het kader van deze Verwerkersovereenkomst inschakelt.
27. Verwerker garandeert Persoonsgegevens en andere informatie verkregen van de Verwerkingsverantwoordelijke strikt geheim te houden. Verwerker zal de Persoonsgegevens of andere informatie verkregen van de Verwerkingsverantwoordelijke niet openbaar maken, distribueren, verstrekken, of op andere wijze bekend maken aan andere personen dan haar werknemers die van de Persoonsgegevens of andere informatie verkregen van de Verwerkingsverantwoordelijke kennis moeten kunnen nemen voor hun werkzaamheden voor de Verwerker en zal deze werknemers pas toegang geven tot de Persoonsgegevens en andere informatie verkregen van de Verwerkingsverantwoordelijke, nadat zij zijn geïnformeerd over het vertrouwelijke karakter van de Persoonsgegevens en andere informatie verkregen van de Verwerkingsverantwoordelijke. Verwerker legt het in deze Overeenkomst bepaalde ook aan haar werknemers op.
28. Verwerker dient Verwerkingsverantwoordelijke zo spoedig mogelijk en in ieder geval uiterlijk binnen 24 uur nadat Verwerker ervan kennis heeft gekregen, in kennis te stellen van iedere inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de Verwerking van Persoonsgegevens.
29. Verwerker dient Verwerkingsverantwoordelijke in ieder geval informatie te verstrekken over het volgende:
30. de aard van de inbreuk, waar mogelijk onder vermelding van de categorieën van Betrokkenen in kwestie en, bij benadering, het aantal Betrokkenen in kwestie;
31. de (mogelijk) getroffen Persoonsgegevens en, bij benadering, het aantal getroffen Persoonsgegevens in kwestie;
32. de vastgestelde en verwachte gevolgen van de inbreuk voor de Verwerking van de Persoonsgegevens en de daarbij betrokken personen; en

33. de maatregelen die Verwerker heeft getroffen en zal treffen om de inbreuk aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele negatieve gevolgen van de inbreuk.
34. Verwerker erkent dat Verwerkingsverantwoordelijke onder omstandigheden wettelijk verplicht is om een inbreuk op de beveiliging (van welke aard dan ook) die (mede) betrekking heeft of kan hebben op de Persoonsgegevens die Verwerker verwerkt, aan Betrokkenen en/of autoriteiten te melden. Een dergelijke melding door Verwerkingsverantwoordelijke zal niet als tekortkoming in de nakoming van deze verwerkersovereenkomst of overeenkomst of anderszins als onrechtmatige handeling worden beschouwd.
35. Verwerker zal alle maatregelen treffen die nodig zijn om de (mogelijke) schade van een inbreuk op de beveiliging te beperken en zal Verwerkingsverantwoordelijke ondersteunen bij meldingen aan Betrokkenen en/of autoriteiten.
36. De aansprakelijkheid van Verwerker is beperkt tot directe schade voortvloeiende uit of verband houdend met het niet-nakomen van deze Verwerkersovereenkomst dan wel handelen in strijd met de toepasselijke Privacywetgeving.
37. Verwerker is niet aansprakelijk voor schade veroorzaakt door het onjuiste gebruik door Verwerkingsverantwoordelijke of schade anderszins veroorzaakt door Verwerkingsverantwoordelijke.
38. De aansprakelijkheid van Verwerker voor door Verwerkingsverantwoordelijke geleden schade en/of verbeurde boetes zoals bedoeld in artikel 11.1 is per gebeurtenis (waarbij een samenhangende reeks van gebeurtenissen telt als één gebeurtenis) beperkt tot vergoeding van schade tot maximaal een bedrag ter hoogte van €50.000. In geen geval zal de totale en cumulatieve aansprakelijkheid onder en in verband met de overeenkomst van een partij jegens de andere partij meer bedragen dan €500.000,-.
39. Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en Verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
40. Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.
41. Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig indien schriftelijk overeengekomen.

Hoofdstuk 10 | **Privacy Statement**

Zoals eerder beschreven is de opdrachtgever van Welder de verwerkingsverantwoordelijke. Als verwerkingsverantwoordelijke is de opdrachtgever verplicht haar medewerkers goed te informeren over de rechten rond privacy. En moeten medewerkers expliciet toestemming geven voor het verwerken van de persoonsgegevens (grondslag 1).

Er zijn drie manieren waarop de opdrachtgever dat kan doen en Welder wijst in iedere samenwerking haar opdrachtgevers op deze drie mogelijke manieren:

Optie 1: De Opdrachtgever neemt in haar arbeidsovereenkomst een passage op waarin hier meer over verteld wordt. De werknemer geeft toestemming door het ondertekenen van het contract.

Optie 2: Er wordt door Opdrachtgever een privacy statement opgesteld en gedeeld met elke medewerker die het Welder platform wil gebruiken. De werknemer moet akkoord gaan met dit privacy statement om gebruik te kunnen maken van het platform.

Optie 3: Opdrachtgever maakt gebruik van het standaard privacy statement van Welder. Deze werkt technisch hetzelfde als optie 2, maar omdat Welder ervaren heeft dat veel bedrijven hier niet op voorbereid zijn, is een vast stramien gemaakt. Dit stramien is hierna te vinden.

In elke samenwerking wordt bepaald welke optie het meest geschikt is voor de opdrachtgever. Bij optie 2 en 3 krijgt elke medewerker wanneer hij of zij voor het eerst gebruik maakt van het Welder platform een geautomatiseerde pop-up waarin gewezen wordt op de privacyrechten. De medewerker kan dan wel of niet toestemming geven op de verwerking van data. De opdrachtgever krijgt inzichtelijk welke mensen wel of geen toestemming hebben gegeven.

Privacy Statement <naam Opdrachtgever>

Ten behoeve van gegevens rond <opdrachtgever>.welder.nl

1. Inleiding

<opdrachtgever> waardeert de privacy van haar medewerkers. Op de website <opdrachtgever>.welder.nl worden gebruikersgegevens verzameld. Om helderheid te geven op welke manier de privacy van bedrijven en werknemers op de website geborgd blijft, is dit privacy statement opgesteld.

De website <opdrachtgever>.welder.nl wordt gebruikt om bijvoorbeeld:

- Intern te communiceren
- Intern onderzoek te doen onder medewerkers
- Ontwikkelgesprekken te voeren
- E-learnings aan te bieden
- Kennis te delen
- Medewerkers begeleiden in hun persoonlijke ontwikkeling

<weghalen wat niet van toepassing is>

2. Welke gegevens worden opgeslagen?

De volgende gegevens worden verwerkt:

- Voor- en achternaam;
- E-mailadres (communicatie met Betrokkene)
- Functie (om competenties aan functie van Betrokkene te koppelen)
- Geboortedatum (om een verjaardag te tonen)
- Leidinggevende (om te weten met wie Betrokkene een voortgangsgesprek voert)
- (evt) Tweede leidinggevende
- Afdeling (om te kunnen selecteren of een gesprekscyclus van toepassing is op Betrokkene)
- In dienst datum (om een jubileum te tonen)
- Uit dienst datum (om een gebruiker te verwijderen)
- Salaris (om het salaris te tonen in een voortgangsgesprek)
- FTE (om het salaris te tonen in een voortgangsgesprek)
- Salarisschaal (om een advies voor salarismutatie te kunnen geven)
- Door de Betrokkene zelf ingegeven scores op zaken als werkgeluk, competenties en doelstellingen. (om leidinggevende en medewerker een gesprek te laten voeren over het functioneren van de medewerker)

3. Waarom worden deze gegevens opgeslagen?

De verschillende persoonsgegevens hebben hun eigen noodzakelijkheid. Sommige persoonsgegevens worden verzameld vanuit een praktisch oogpunt. Zonder bijvoorbeeld een emailadres kunnen we een medewerker geen uitnodiging sturen voor een medewerkersonderzoek. Andere persoonsgegevens worden verzameld om de juiste inzichten te verzamelen voor een strategische personeelsplanning. Zo worden leidinggevenden gevraagd informatie te geven over het ingeschatte potentieel van medewerkers gebruikt voor automatische analyses door het management van de opdrachtgevers. Tenslotte worden persoonsgegevens verwerkt om de medewerker te

helpen bij de persoonlijke ontwikkeling. Zo kan een medewerker tijdens de voorbereiding van een functioneringsgesprek inzicht geven in de persoonlijke werktevredenheid. Deze data moet verzameld en verwerkt worden, zodat leidinggevende en medewerker samen tijdens het gesprek een actieplan kunnen maken rond de persoonlijke ontwikkeling van medewerkers.

Leverancier van het platform <naam platform> is Welder.

Naam	WELDER
KvK	84324627
Branche	Adviesorganisatie
Adres	Bremvallei 1, 5237 LV ‘s-Hertogenbosch
E-mail	info@welder.nl
Website	www.welder.nl
Telefoon	073-2082800

<opdrachtgever> heeft met Welder afspraken gemaakt over de verwerking van persoonsgegevens. Deze zijn vastgelegd in een verwerkersovereenkomst, die is op te vragen door een e-mail te sturen aan info@welder.nl. De gegevens van het gebruik van <naam platform> worden opgeslagen bij hostingpartij Hetzner te Duitsland.

4. Hoe lang worden jouw persoonsgegevens bewaard?

Gebruiksgegevens worden opgeslagen op de servers van Welder gedurende de looptijd van het contract met <naam opdrachtgevers>. <Naam opdrachtgever> heeft met Welder afgestemd dat persoonsgegevens ouder dan <periode> worden verwijderd.
<verwijderen wat niet van toepassing is>

5. Wat zijn jouw rechten?

Betrokkenen, medewerkers van <naam opdrachtgever>, hebben diverse rechten met betrekking tot de gegevens. In deze privacyverklaring geeft <naam opdrachtgever> jou informatie over je privacy rechten voor het gebruik van <naam platform>. Daarnaast heb je het recht om in te zien of een kopie te ontvangen van de persoonsgegevens die in <naam platform worden verwerkt. Staan er fouten in het systeem? Dan heb je het recht deze te laten wijzigen. Als er geen grond (meer) bestaat om bepaalde gegevens te bewaren, dan heb je het recht om deze gegevens te laten verwijderen. Een verzoek tot inzage, wijziging, verwijdering of kopie kun je indienen bij info@welder.nl / <contactgegevens opdrachtgever>.

Tot slot wijst <naam opdrachtgever> je op de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens. Meer informatie vind je op www.autoriteitpersoonsgegevens.nl.

6. Beveiliging

<Naam opdrachtgever> neemt de bescherming van jouw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als je de indruk hebt dat de

gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, kun je het beveiligings- en privacybeleid van Welder opvragen. Deze is vrij te downloaden op www.welder.nl.

7. Vragen

Bij vragen over dit privacy statement kan men zich wenden tot info@welder.nl / contactgegevens opdrachtgever>.

Hoofdstuk 11 | **Roadmap ISO-certificering**

In 2025 is Welder gestart met het certificeringstraject voor ISO-27001. Samen met een extern bureau is een roadmap opgesteld om certificering in 2026 mogelijk te maken.

Roadmap:



Hoofdstuk 12 | **Resultaten interne toets**

Alle medewerkers van Welder dienen tweejaarlijks een privacytoets te doorlopen. Dit is een E-learning met 10 vragen die opgesteld worden door de privacy officer en functionaris gegevensbescherming van Welder. Hieronder de vragen en resultaten van de laatste interne toets in 2025.

1. Wie is de verwerkersverantwoordelijke in onze contracten met opdrachtgevers?
   - [x] Onze klant
   - [ ] Welder
   - [ ] De eindgebruiker
   - [ ] De leidinggevende

2. Wat is de rol van Welder ten aanzien van gegevensverwerking?
   - [ ] Gegevensbeheerder
   - [x] Verwerker
   - [ ] Verwerkingsverantwoordelijke
   - [ ] Systeemgebruiker

3. Wat is de standaard grondslag voor het verwerken van persoonsgegevens door Welder?
   - [ ] Gerechtvaardigd belang
   - [ ] Wettelijke verplichting
   - [x] Toestemming
   - [ ] Uitvoering van een overeenkomst

4. Welke route mag NIET gebruikt worden voor het aanleveren van persoonsgegevens van medewerkers?
   - [ ] A. Een automatische koppeling
   - [ ] B. Handmatige invoer door Eindgebruiker
   - [ ] C. Upload via documentenportaal
   - [x] D. Verzenden via e-mail

5. Wat moet Welder doen als een medewerker van de opdrachtgever verzoekt om zijn of haar gegevens te verwijderen?
   - [ ] A. Dit verzoek doorsturen naar de directie
   - [ ] B. Overleggen met de leidinggevende
   - [x] C. Dit verzoek altijd honoreren
   - [ ] D. Dit verzoek pas uitvoeren bij opzegging van het contract

6. Waar worden de gegevens van Eindgebruikers fysiek opgeslagen?
   - [ ] A. In een eigen datacenter in Nederland
   - [ ] B. Bij een externe cloudprovider buiten de EU
   - [x] C. In een ISO-gecertificeerd datacenter in Duitsland
   - [ ] D. Lokaal op Welder-laptops

7. Hoe weet een Eindgebruiker dat er gegevens van hem/haar worden verwerkt in het platform?

- [ ] Via een mail van de privacy officer
- [x] Door het privacy statement bij eerste gebruik
- [ ] Door een vermelding in zijn of haar contract
- [ ] Door een bericht van de leidinggevende

8. Wat geldt er bij beëindiging van het gebruik van de Welder software?

- [ ] Alle data wordt per direct automatisch verwijderd
- [ ] Gebruikersdata moet verplicht worden bewaard
- [x] De opdrachtgever mag vragen om verwijdering van de data
- [ ] Alleen financiële gegevens worden overgedragen

9. Wat moet je doen bij het vermoeden van een datalek?

- [ ] Zelf het probleem proberen op te lossen en afwachten
- [ ] Binnen 24 uur melden bij de Opdrachtgever
- [x] Binnen 24 uur melden bij de privacy officer van Welder
- [ ] Het delen met collega's om te bespreken wat te doen

10. Wat geldt volgens de verwerkersovereenkomst van Welder over aansprakelijkheid bij een datalek?

- [ ] Welder is altijd volledig aansprakelijk voor alle kosten
- [ ] Alleen de opdrachtgever draagt verantwoordelijkheid
- [x] Welder is aansprakelijk tot een maximum van €50.000 per incident
- [ ] Bij een datalek zijn er nooit financiële gevolgen

Naam	Resultaat	Naam	Resultaat
Anouk van der Pol	Geslaagd	Marco Kuis	Geslaagd
Brianne Kappen	Geslaagd	Martijn Cuijten	Geslaagd
Daan Derks	Geslaagd	Michael Mannien	Geslaagd
Ferry van Hooydonk	Geslaagd	Myra van Schijndel	Geslaagd
Fleur van den Berg	Geslaagd	Nan van Lith	Geslaagd
Gijs Groothuis	Geslaagd	Nikki Vlemmings	Geslaagd
Hein vd Kerkhof	Geslaagd	Quinty van Riel	Geslaagd
Jack Pastora	Geslaagd	Renee van Drunen	Geslaagd
Jari van Galen	Geslaagd	Richard Palm	Geslaagd
Jelle Staal	Geslaagd	Rob Wouters	Geslaagd
Jeroen Jansen	Geslaagd	Sander Peters	Geslaagd
Karlijn van Kessel	Geslaagd	Stefan Boenders	Geslaagd
Kiki Vonk	Geslaagd	Sven Huirne	Geslaagd
Linda de Rooij	Geslaagd	Thirza Veenstra	Geslaagd
Liza Maas	Geslaagd		
Luuk Sanders	Geslaagd		
Maarten Schellekens	Geslaagd		