Mangaan 4 B
5234 GD
‘s-Hertogenbosch

KvK: 84324627
073 208 2800
www.welder.nl
info@welder.nl

Beveiligings- en privacybeleid WELDER

Versie: april 2023

WELDER

Inhoud

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 kiezen we voorlopig niet voor bijvoorbeeld een ISO certificering. 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 gebrekken 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 hierarchisch 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 getoetst door een extern bureau. De laatste toets dateert van maart-2022 en is uitgevoerd door 'De Functionaris' (kvk: 69175829). Resultaten van deze externe toets zijn op aanvraag (info@welder.nl) inzichtelijk.

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 korte samenvatting van essentiele punten uit het Beveiligings- en privacybeleid.
- Verwerkersovereenkomst | Hierin worden op basis van het Beveiligings- en privacy beleid 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 o.a. verwachtingen van WELDER naar de medewerkers tav beveiliging en privacy vastgelegd.

3.2 Autorisatiemodel

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

	Gebruik van WELDER software	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
Overige WELDER medewerkers	x			x	x
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 saparaat 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 (2023: Ferry van Hooydonk)	Signaleren van afwijkingen aan het privacy beleid. Up-to-date houden van het privacy beleid. Rapporteren aan directie over naleving privacy beleid.
Developers WELDER	Beheer en ontwikkeling technische maatregelen rond privacy.
Accountmanagers WELDER	Communicatie naar Opdrachtgevers in kader privacy beleid.
Directie WELDER (Rob Wouters, Maarten Schellekens)	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 privacy officer krijgt een signaal hiervan, kan evalueren of dit de juiste data is en deze doorsturen aan de betreffende accountmanager. Zo voorkomen we dat dergelijke persoonsgegevens terecht komen bij mensen waarvoor deze niet bedoeld zijn.

3.8 Toestemming beeldmateriaal

Elke medewerker van WELDER heeft in de arbeidsovereenkomst opgenomen dat eventueel opgenomen beeldmateriaal van de medewerker wordt gebruikt in externe communicatie.

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 geevalueerd door de functionaris Gegevensbescherming van WELDER en in overleg met directie WELDER geupdatet.

Hoofdstuk 4 | Verwerkingsregister

4.1 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 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	Noodzakelijk zodat Eindgebruikers elkaar kunnen feliciteren met de verjaardag en sommige Opdrachtgevers kiezen ervoor een ontwikkelgesprek te voeren rond een verjaardag.
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.
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.
Telefoonnummer	Noodzakelijk zodat Eindgebruikers elkaar snel kunnen bereiken telefonisch.
Taal	Noodzakelijk zodat helder is in welke taal de WELDER software getoond moet worden.

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.

4.3 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 binnen komt bij de Privacy Officer van WELDER. Zo beperken we het risico dat een medewerker per ongeluk een mail doorstuurt.

4.4 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.

4.5 Subverwerkers

WELDER heeft momenteel één subverwerker (Hetzner te Duitsland als hosting partner) en garandeert dat dergelijke subverwerkers een soortgelijk verwerkingsregister vastleggen met contactgegevens.

4.6 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

WELDER gaat in principe uit van grondslag 1: toestemming. Elke Eindgebruiker wordt bij het eerste gebruik gewezen middels een pop-up op een privacy statement waarin verwezen wordt naar die beveiligings- en privacybeleid. De Eindgebruiker kan enkel gebruik maken van het platform wanneer hij of zij hiermee akkoord gaat en dus toestemming geet over het verwerken van de persoonsgegevens.

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

De toestemming moet door de Eindgebruiker vrijelijk gegeven kunnen worden; een Eindgebruiker moet bij het weigeren niet gehinderd worden in het uitvoeren van de arbeidsovereenkomst. Dit wordt gecommuniceerd met de Opdrachtgevers van WELDER.

Er zijn Opdrachtgevers die in hun arbeidsovereenkomst met Eindgebruikers duidelijke afspraken hebben opgenomen over het gebruik van bedrijfssoftware. In dat geval kan ervoor gekozen worden grondslag 2 (uitvoeren overeenkomst) te hanteren en zal geen pop-up verschijnen bij het eerste gebruik van de WELDER software. Per Opdrachtgever wordt de juiste grondslag vastgesteld.

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-april 2022 bedraagt het aantal gebruikers van WELDER ca. 47.000.

5.3 Privacy by Desgn 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 en de code hierna over te dragen aan opdrachtgever. 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, heeft opdrachtgever het recht gebruikersdata te laten 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.
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)
Elke nacht wordt er een back-up gemaakt, waarmee maximaal dataverlies een dag bedraagt. In overleg zou dit ingekort kunnen worden.

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

In ruste is gevoelige data (wachtwoordhashes) encrypted, gedurende verzending via HTTPS.

5.26 Opslag binnen EU

Hetzner datacenter in Falkenstein. Opslag/verwerking binnen EU wordt gegarandeerd.

Hoofdstuk 6 | Data Protection Impact Assessment (DPIA)

Door: WELDER
Datum uitvoering: mei 2022

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 hoofdstuk 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 bijvoorbeeld de naam en het e-mailadres van de medewerker 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 elkens 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 | Externe toets door Computest

WELDER laat periodiek een externe toets rond beveiliging uitvoeren door een extern bedrijf. De laatste resultaten daarvan zijn openbaar voor alle klanten. De laatste scan is uitgevoerd door het bedrijf Computest en werd uitgevoerd in het kader van het officiële partnership met softwarebedrijf AFAS.

Computest werkt met een kleurcodering:

- Rood: afgekeurd
- Oranje: een aantal verbeterpunten, nieuwe audit over één jaar
- Groen: goed op orde, nieuwe audit over 3 jaar

In de laatste check van 25 maart 2022 werd de groene score behaald, hetgeen WELDER vertrouwen geeft dat de beveiliging cq privacy van data goed geborgd is.

WELDER

Computest

Partner Security Quickscan
WELDER B.V.

>>

WE EAT SECURITY FOR BREAKFAST.

25 maart 2022
Michael de Klein

Samenvatting

Op 23 en 24 maart 2022 heeft Computest een security quickscan uitgevoerd voor WELDER. Hiervoor heeft Michael de Klein, securityspecialist bij Computest, gesproken met Rob Wouters en Stefan Boenders, ontwikkelaars bij WELDER, over de beveiliging van de WELDER HRM applicatie. Ook heeft Computest kort gekeken naar de broncode van de applicatie en een korte securitytest uitgevoerd.

Het doel van een quickscan is om een idee te geven van de staat van beveiliging van de WELDER HRM applicatie. Dit document geeft dan ook alleen een algemene indruk, en is geen volledige opsomming van alle kwetsbaarheden in de applicatie.

De WELDER HRM applicatie biedt bedrijven een omgeving waarin het sociale aspect centraal staat. In de applicatie kunnen middels een berichtenbord berichten gedeeld worden met collega's en leidinggevenden. Verder bevat de applicatie de mogelijkheid om competenties te koppelen aan medewerkers en deze competenties te toetsen door middel van een functioneringsgesprek, welke allemaal gedocumenteerd kunnen worden binnen het platform. Verder biedt het platform ook de mogelijkheid om e-learning modules te maken welke gebruikt kunnen worden voor bijvoorbeeld on- of off-boarding doeleinden of andere kennisdeling doeleinden. Middels een marktplaats module is het voor medewerkers mogelijk om voorwerpen, diensten of doelen te delen binnen een organisatie, of punten toe te kennen aan goede doelen.

De applicatie gebruikt werknemer data uit het AFAS-systeem om bijbehorende accounts aan te maken binnen het platform, zodat iedere (nieuwe) werknemer hier toegang toe heeft. Daarnaast is het mogelijk na het afronden van een gesprek om hiervan een verslag op te slaan bij een werknemer in het AFAS-systeem.

Resultaat

Op basis van de vier onderstaande pijlers zijn scores toegekend. Verder in dit document lichten wij elke onderwerp nader toe:

Scoreverdeling	
Security in het ontwikkelproces	
Security in code	
Security in de praktijk	
Risico voor AFAS	

Het risico voor AFAS heeft een groen stoplicht gekregen. AFAS verwacht dat er na 3 jaar een vervolgafspraak wordt gemaakt.

Security in het ontwikkelproces

Er is ruimte voor verbetering voor security in het ontwikkelproces.

Computest heeft gesproken met ontwikkelaars van WELDER over de ontwikkeling van de HRM applicatie. Hieruit is gebleken dat op veel onderdelen in het ontwikkelproces er aandacht is voor security gezien de omvang van het team, maar dat er nog wel een aantal verbeteringen mogelijk zijn. Binnen WELDER zijn er op het moment vier ontwikkelaars werkzaam, welke allemaal aan dezelfde applicatie werken. De applicatie is gebouwd met een AngularJS front-end en Python Pyramid als back-end framework, en is gebouwd als multi-tenant omgeving. De achterliggende database bevat alle data van alle WELDER-klanten en wordt op data-niveau van elkaar onderscheiden. Bij het inrichten van omgevingen voor nieuwe klanten wordt er gevraagd naar de AFAS-token van de klant, waarvoor geen vastgestelde procedure is opgesteld naar hoe de klant dit token zou moeten aanleveren.

Omdat alle ontwikkelaars werken aan dezelfde applicatie en daarom ook allemaal gebruik maken van dezelfde diensten (infrastructuur, databases, ed.) is hierin geen onderscheid gemaakt in wie toegang heeft tot welke componenten. Wel wordt er op de servers afgedwongen dat enkel IP-adressen van ontwikkelaars in combinatie met '*SSH Public key authentication*' mogen verbinden naar de servers.

Op de GitLab code repository wordt veel aandacht besteed aan code kwaliteit en peer reviewing. Zo worden nieuwe functies ontwikkeld in een aparte branch en worden er code reviews uitgevoerd worden op alle nieuwe merge requests om alle toegevoegde code te beoordelen. Er is echter geen proces dat dit afdwingt, maar wordt gedaan op eigen initiatief van de ervaren ontwikkelaars. Daarnaast worden er in de deployment pipeline tests uitgevoerd op de code, en worden dependencies van de software gescand op publiek bekende kwetsbaarheden. Alle interne accounts (tot bijvoorbeeld de broncode) zijn beschermd met een Google SSO oplossing welke Multi-factor authenticatie (2FA) afdwingt. Door deze maatregelen is het ontwikkelproces voldoende beschermd. Wel is er een klein risico doordat alle ontwikkelaars in het team toegang hebben tot de productieomgeving van de applicatie. Als een aanvaller toegang weet te krijgen tot het systeem van een van deze ontwikkelaars, is het mogelijk dat de aanvaller daarmee toegang tot de productieomgeving weet te krijgen. Daarnaast is er geen proces waarmee WELDER controleert of de systemen van de ontwikkelaars voldoende beveiligd zijn, door bijvoorbeeld te controleren of updates zijn geïnstalleerd, disk encryptie aanstaat en of een virusscanner actief is.

Op basis van bovenstaande informatie adviseert Computest:

- Richt een proces in waarmee inzicht verkregen kan worden in de beveiliging van alle werkstations;
- Stel een procedure in voor het ontvangen van AFAS-tokens, bijvoorbeeld versleuteld per mail met het wachtwoord per sms;
- Isoleer databases van elkaar zodat er bij een security kwetsbaarheid extra isolatie aanwezig is tussen klanten;
- Sla het AFAS-token versleuteld op in de database zodat deze bij een lek niet uitgelezen en/of misbruikt kan worden;
- Beperk het aantal personen dat toegang heeft tot de productie-infrastructuur.

Security in code

Er is voldoende aandacht voor security in de broncode van de applicatie(s).

Computest heeft samen met de ontwikkelaar van WELDER gekeken naar de broncode van de HRM applicatie. De applicatie is geschreven in Python in combinatie met het Pyramid framework. Dit wordt gedaan op een overzichtelijke wijze, en alle code wordt zo geschreven dat de functionaliteiten en waarden zichzelf zo helder mogelijk omschrijven. Alle externe softwarepakketten die worden ingeladen worden in de CI/CD pipeline gecontroleerd op publiekelijk bekende kwetsbaarheden en de teststraat zal falen wanneer deze aangetroffen worden. Alle routes binnen de applicatie worden op object niveau ingeladen en hier worden ook authenticatie checks op een gecentraliseerde manier afgehandeld.

Voor communicatie met de database wordt gebruik gemaakt van het softwarepakket *sqlalchemy* dat gebruik maakt van '*Object-relational mapping (ORM)*' waardoor er geen gebruik gemaakt hoeft te worden van SQL-queries. Hiermee biedt het *sqlalchemy* softwarepakket beveiliging tegen SQL-injectie.

Ook is er structureel bescherming aanwezig tegen '*Cross-Site Scripting (XSS)*' doordat hiervoor in zowel de front- als back-end gebruik gemaakt wordt van functies die gebruikersinvoer filteren. In combinatie met deze beschermende maatregelen heeft WELDER ook een zeer stricte '*Content Security Policy (CSP)*' ingesteld zodat er in het geval van een incidentele XSS-kwetsbaarheid een extra laag van bescherming aanwezig is.

Verder lijkt er geen bescherming geboden te worden tegen '*Cross-Site Request Forgery (CSRF)*'. Er worden bij POST-verzoeken geen gebruik gemaakt van CSRF-tokens waardoor het voor een aanvaller mogelijk zou zijn om een dergelijke aanval uit te voeren. Tijdens de code review heeft Computest deze kwestie besproken met de ontwikkelaar, welke aangaf dat er beschermd wordt tegen CSRF door op het sessie-cookie de '*Same-Site*' vlag een '*Lax*' waarde mee te geven. Omdat er in een aantal gevallen toch een sessie-cookie meegestuurd zal worden bij een Lax Same-Site waarde, heeft Computest ook deze uitzonderingen onderzocht samen met de ontwikkelaar. Hieruit is geconcludeerd dat er in eerste oogopslag geen sprake is van uitzonderingsgevallen waarin een CSRF aanval toch reëel zou zijn. Omdat Same-site nog niet overal ondersteund wordt adviseert Computest toch een extra CSRF-beschermingsmaatregel te overwegen.

Op basis van het bovenstaande adviseert Computest:

- Onderzoek de implementatie van CSRF-tokens in de applicatie om een extra laag van bescherming in te bouwen tegen Cross-Site Request Forgery aanvallen;
- Documenteer de codebase zodat deze voor nieuwe en de huidige ontwikkelaars beter te begrijpen is;
- Bouw in de bestaande CI/CD pipeline SAST en/of DAST tools in zodat hier ook op applicatie niveau beter inzicht verkregen wordt op het security-niveau.

Security in de praktijk

Er is voldoende aandacht voor security in de praktijk.

Tijdens het assessment heeft Computest het securityniveau van de WELDER HRM applicatie beoordeeld. Computest is van mening dat de omgeving voldoende beveiligd is, maar ziet op enkele plekken ruimte voor verbetering om het securityniveau verder te verhogen.

Tijdens de demo van de applicatie heeft Computest bevonden dat er AFAS-tokens onversleuteld worden getoond in het configuratie interface van de applicatie. Computest adviseert om dit token enkel gemaskeerd of helemaal niet te tonen in de applicatie, en deze in de database versleuteld op te slaan.

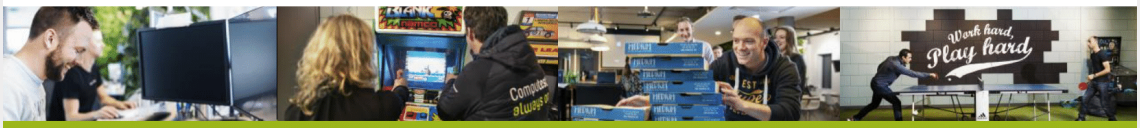
Hoewel er in de code structureel bescherming aanwezig is tegen XSS-kwetsbaarheden, heeft Computest op twee plekken in de applicatie toch een incidentele XSS-kwetsbaarheid aangetroffen. Beide kwetsbaarheden zijn aangetroffen in het formulier waar managers functioneringsgesprekken in documenteren, allereerst in de velden waar managers opmerkingen achter kunnen laten bij een behaald doel, en daarnaast in de pop-up die getoond wordt wanneer een manager het formulier wilt opslaan en de naam van de medewerker getoond wordt. Hoewel Computest geen werkende '*Proof-of-Concept*' heeft van een mogelijke exploitatie, is deze bevinding tijdens het assessment gecommuniceerd met WELDER die dit zal controleren en oplossen. Computest adviseert om de applicatie te controleren op het tonen van gebruikersinvoer om te valideren dat alle incidentele XSS-kwetsbaarheden opgelost zijn.

Risico voor AFAS

Het securityrisico voor AFAS wordt ingeschat op 'Laag'.

De WELDER HRM applicatie maakt gebruik van werknemer data uit AFAS voor het aanmaken van accounts in de omgeving, en zal enkel bij het afronden van een vastgelegd gesprek een gespreksverslag terug uploaden naar AFAS.

In de applicatie heeft Computest geen kritieke kwetsbaarheden aangetroffen en heeft ook geen verdere aanleiding gevonden om te geloven dat de confidentialiteit, integriteit of beschikbaarheid van het AFAS-token, dan wel data afkomstig uit AFAS, op enig manier geschaad kan worden. Computest schat het risico voor AFAS daarom in op 'laag'.



Computest
always on.

info@computest.nl
+31(0)88 733 13 37
www.computest.nl

We zijn een team van gepassioneerde en ervaren technisch specialisten die applicaties en infra-struc-turen optimaal laten werken. Wij geloven in geïntegreerde quality assurance en bieden daarom diensten op het gebied van performance, security en functionele testautomatisering.

In alles wat we doen worden we gedreven door een grenzeloze passie voor kwaliteit. Daarom werken we voor iedere sector samen in kleine, gespecialiseerde agile teams. Daarmee houden we de lijnen kort zodat we de beste resultaten behalen.

Hoofdstuk 8 | Verwerkersovereenkomst

Versie september - 2022

Verwerkersovereenkomst: _____
Datum: _____
Contractspartijen:
1. _____, statutair gevestigd te _____
aan het adres _____ ingeschreven in het handelsregister onder nummer_____, vertegenwoordigd door _____
hierna te noemen: “Verwerkingsverantwoordelijke”,

en

2. WELDER B.V., statutair gevestigd te (5234 GD) ’s-Hertogenbosch aan het adres Mangaan 4 B ingeschreven in het handelsregister onder nummer 84324627 en hierbij rechtsgeldig vertegenwoordigd door M.L.H. Schellekens, mede tekenend namens zichzelf; hierna te noemen: “Verwerker”,

Verwerkingsverantwoordelijke en Verwerker hierna gezamenlijk ook aan te duiden als: “Partijen”;

Overwegende dat:
Partijen hebben een overeenkomst met betrekking tot _____
hierna: de “Overeenkomst”) gesloten. Ter uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

Deze Overeenkomst leidt ertoe dat Verwerker in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens verwerkt. Verwerkingsverantwoordelijke en Verwerker wensen in deze overeenkomst de rechten en verplichtingen voor de Verwerking van Persoonsgegevens door Verwerker vast te leggen overeenkomstig het bepaalde artikel 28 lid 3 Algemene Verordening Gegevensbescherming.

Artikel 1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1.1. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke
persoon („de Betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die
direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke,

fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

1.2. Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel
van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren,
afschermen, wissen of vernietigen van gegevens;

1.3. Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de Persoonsgegeven betrekking hebben;

1.4. Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen ("Verwerkersovereenkomst");

1.5. Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;

1.6. Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde
verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins
verwerkte gegevens ("Datalek");

1.7. Gegevensbeschermingseffectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de Persoonsgegevens;

1.8. Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

1.9. AVG: de Algemene Verordening Gegevensbescherming *(2016/679/EU)*;

1.10. Privacywetgeving: alle toepasselijke wet-en regelgeving op het gebied van privacy waaronder, maar niet beperkt tot de AVG.

Artikel 2. Totstandkoming, duur en beëindiging

2.1. Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.

2.2. Deze Verwerkersovereenkomst is voor onbepaalde tijd aangegaan en eindigt op het tijdstip dat de Overeenkomst eindigt.

2.3. In geval van beëindiging van de Verwerkersovereenkomst zal Verwerker alle Persoonsgegevens overdragen aan Verwerkingsverantwoordelijke, of, op uitdrukkelijk schriftelijk verzoek van Verwerkingsverantwoordelijke de Persoonsgegevens die Verwerker onder zich heeft vernietigen.

2.4. Verplichtingen die naar hun aard bestemd zijn om ook na beëindiging van de Verwerkersovereenkomst voort te duren, blijven na beëindiging gelden. Tot deze

verplichtingen behoren onder meer de bepalingen betreffende geheimhouding, overdracht en vernietiging, aansprakelijkheid en toepasselijk recht.

Artikel 3. Verwerken Persoonsgegevens

3.1. 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.

3.2. Verwerker Verwerkt de Persoonsgegevens slechts in opdracht van Verwerkingsverantwoordelijke, tenzij afwijkende wettelijke verplichtingen gelden.

3.3. 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.

3.4. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk schriftelijk in kennis indien een instructie naar het redelijk oordeel van Verwerker inbreuk oplevert op de toepasselijke privacywetgeving.

3.5. 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.

3.6. 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.

3.7. 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.

3.8. Verwerker mag de Persoonsgegevens enkel buiten de EER Verwerken met voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke.

Artikel 4. Beveiligen van Persoonsgegevens

4.1. 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 bijlage (beveiligings- privacybeleid WELDER)

4.2. Verwerker informeert Verwerkingsverantwoordelijke indien een van de beveiligingsmaatregelen wijzigt.

4.3. Verwerker staat toe dat Verwerkingsverantwoordelijke de naleving van de beveiligingsmaatregelen door Verwerker inspecteert of dat op verzoek van

Verwerkingsverantwoordelijke de gegevensverwerkingsfaciliteiten van Verwerker door een door Verwerkingsverantwoordelijke 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.

4.4. Verwerkingsverantwoordelijke zal alle kosten, vergoedingen en onkosten in verband met de inspectie betalen, met inbegrip van redelijke door Verwerker gemaakte interne kosten.

4.5. Verwerkingsverantwoordelijke zal Verwerker een exemplaar van het rapport van de inspectie verstrekken.

Artikel 5. Verstrekking Persoonsgegevens aan derden

5.1. 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.

5.2. Verwerker zal Verwerkersverantwoordelijke schriftelijk om toestemming vragen om Persoonsgegevens aan derden te vertrekken en hiertoe pas overgaan na schriftelijke toestemming van Verwerkersverantwoordelijke.

5.3. 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.

Artikel 6. Verzoeken van Betrokkenen

6.1. 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.

6.2. Verwerker handelt alle verzoeken om inlichtingen van Verwerkingsverantwoordelijke met betrekking tot de Verwerking van de Persoonsgegevens vlot en behoorlijk af conform de AVG.

Artikel 7. Medewerking Verwerker

Verwerker zal de Verwerkingsverantwoordelijke medewerking verlenen bij het doen nakomen van de verplichtingen om:

i. verzoeken van Betrokkenen met betrekking tot de uitoefening van rechten van Betrokkenen op grond van de toepasselijke Privacywetgeving te beantwoorden;
ii. passende technische en organisatorische maatregelen te nemen om een op het risico afgestemd beveiligingsniveau te waarborgen;
iii. datalekken te melden aan toezichthouder en de betrokkenen;
iv. een Gegevensbeschermingseffectbeoordeling uit te voeren;
v. de toezichthouder te raadplegen voorafgaand aan een Verwerking de een hoog risico met zich meebrengt.

Artikel 8. Inschakelen sub-verwerkers door Verwerker

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.

Artikel 9. Geheimhouding

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.

Artikel 10. Datalekken

10.1. 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.

10.2. Verwerker dient Verwerkingsverantwoordelijke in ieder geval informatie te verstrekken over het volgende:

i. de aard van de inbreuk, waar mogelijk onder vermelding van de categorieën van Betrokkenen in kwestie en, bij benadering, het aantal Betrokkenen in kwestie;

ii. de (mogelijk) getroffen Persoonsgegevens en, bij benadering, het aantal getroffen Persoonsgegevens in kwestie;

iii. de vastgestelde en verwachte gevolgen van de inbreuk voor de Verwerking van de Persoonsgegevens en de daarbij betrokken personen; en

iv. 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.

10.3. 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.

10.4. 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.

Artikel 11. Aansprakelijkheid

11.1. 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.

11.2. Verwerker is niet aansprakelijk voor schade veroorzaakt door het onjuiste gebruik door Verwerkingsverantwoordelijke of schade anderszins veroorzaakt door Verwerkingsverantwoordelijke.

11.3. 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,-.

Artikel 12. Slotbepalingen

12.1. Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.

12.2. Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de
Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.

12.3. Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig indien schriftelijk overeengekomen.

12.4. Op deze Verwerkersovereenkomst is Nederlandse recht van toepassing.

12.5. Alle geschillen voortvloeiende uit of samenhangende met deze Overeenkomst zullen uitsluitend worden voorgelegd aan de bevoegde rechter te ‘s-Hertogenbosch.

Bijlage: Beveiligings- en privacy beleid WELDER (versie april 2023)

Aldus door ons overeengekomen en ondertekend:

Verwerkingsverantwoordelijke:

Ondertekend voor en namens: _____
Naam: _____
Functie: _____
Datum en plaats: _____

Handtekening:

Verwerker:

Ondertekend voor en namens: WELDER B.V.
Namen: Maarten L.H. Schellekens
Functie: Directie
Datum en plaats: _____

Handtekening
M.L.H.
Schellekens:

Hoofdstuk 9 | 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	Mangaan 4B, 5234 GD ‘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>.