

AVG proof quickscan

Applicant Tracking Systemen

2018

Vraag #	% Ja	% Nee	% Roadmap	% Anders
12. Automatische toestemming vragen aan aspirant kandidaat				
13. Exporteren voorgeschreven verwerkingsregister				
14. Geautomatiseerd matchen				
14a. DPIA rapport beschikbaar	10	90		



Inhoud

1. Inleiding en context.....	3
2. Respondenten	6
3. Globale resultaten	7
4. Resultaten per vraag.....	8
5. Conclusies en mogelijke vervolgstappen.....	10
6. Scores per leverancier	11
Actief software	11
Carerix	14
Connexys by Bullhorn	17
Cornerstone	20
HROffice.....	25
Oracle Taleo	28
Otys.....	31
Talentsoft.....	35
Tangram	37
Visma.....	40
Bijlage 1 AVG-artikelen die gebruikt zijn voor de quickscan vragen.	42
Bijlage 2 Verwerkingsregister en DPIA	49
Disclaimer	52
Over de auteurs.....	53

Inleiding en context

Het rapport AVG proof quickscan Applicant Tracking Sytemen (ATS) 2018 is het resultaat van een steekproef onder de ongeveer 40 in Nederland actieve leveranciers, die ondersteuning bieden voor het wervings-, selectie- en contracteringsproces.

De quickscan is in januari 2018 uitgevoerd en de resultaten zijn gepresenteerd tijdens het op 14 februari 2018 gegeven webinar "Hoe ga je om met persoonsgegevens tijdens de werving."

Kijk voor meer informatie over het webinar op:
<https://vroomhr.nl/webinar-avg-en-persoonsgegevens/>

Quickscan vragen en antwoord opties

De vragen in de quickscan zijn gebaseerd op de Algemene Verordening Gegevensbescherming (AVG) die op 25 mei 2018, de huidige Wet Bescherming Persoonsgegevens (WbP) vervangt. Voor informatie over de AVG verwijzen wij naar de site van de Autoriteit Persoonsgegevens.

De AVG-proof quickscan ATS 2018 bevat vragen die gebaseerd zijn op een select aantal artikelen uit de AVG, die impact hebben op de manier waarop recruiters werken. Voor een overzicht van deze artikelen verwijzen wij naar bijlage 1 van dit rapport.

De betreffende artikelen zijn vertaald naar 14 hoofdvragen over functionaliteiten van het ATS, waarmee de recruiter ondersteund wordt bij het waarborgen van de privacy van de sollicitant.

Respondenten konden kiezen uit de antwoord opties:

- Ja
- Nee
- Op roadmap
- Anders, namelijk

Omdat er nog veel discussie is over de praktische uitwerking van de AVG, hebben wij respondenten aangemoedigd bij antwoord optie "Anders, namelijk.." commentaar te geven, als zij een andere interpretatie van het betreffende AVG-artikel hanteerden, dan Vroom Consultancy.

Een aantal respondenten heeft hier gebruik van gemaakt.

Proces scope

In het stripverhaal hieronder staat in grote stappen de proces scope van de quickscan geschetst; van vacature opstellen tot en met de aanstelling. De vragen gaan in op een aantal momenten in dit proces, te weten:

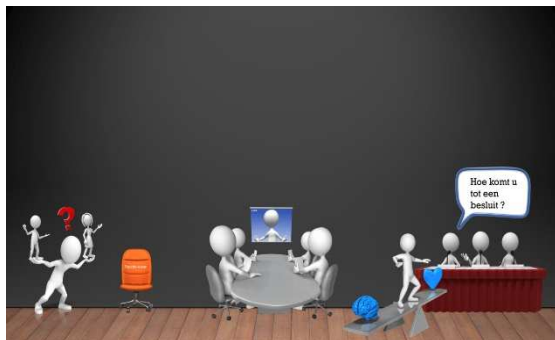
Het verkrijgen van toestemming van zowel personen die solliciteren, als van personen van wie het profiel gevonden wordt omdat de recruiter hier zelf naar op zoek gaat(sourcing).



Van functie eisen naar eerste reacties en actieve search



Geautomatiseerd matchen



Aanbod en gesprekken



Assessments en aanbieden arbeidsovereenkomst

Geautomatiseerd matchen van cv's met de vacature eisen en de bestaande en nieuwe rechten van kandidaten vanuit de AVG:

- Vergetelheid; het recht om 'vergeten' te worden (NIEUW).
- Inzage; het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
- Rectificatie en aanvulling; het recht om de persoonsgegevens die u verwerkt te wijzigen.
- Beperking van de verwerking; het recht om minder gegevens te laten verwerken.
- Voorwaarden met betrekking tot geautomatiseerde besluitvorming en profilering; het recht op een menselijke blik bij besluiten.
- Het recht om bezwaar te maken tegen de gegevensverwerking.
- Dataportabiliteit; het recht om persoonsgegevens over te dragen (NIEUW).
- Duidelijke informatie over wat u met de gegevens doet en of u ze eventueel doorgeeft aan anderen.

- Het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde matching van cv's met functieprofielen gebaseerd besluit, waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Dit recht beoogt onterechte afwijzing voor een passende vacature te voorkomen.

Respondenten

Onderstaande leveranciers hebben de quickscan ingevuld.



The image shows a presentation slide with a dark background and a wooden floor at the bottom. The title 'RESPONDENTEN' is centered at the top in orange. Below it is a table with two columns and ten rows, listing suppliers. The table has an orange header and footer row. The suppliers listed are: 1. ActiefSoftware, 2. Carerix, 3. Connexys by Bullhorn, 4. Cornerstone, 5. HROffice, 6. Oracle Taleo, 7. Otys, 8. Talentsoft, 9. Tangram, and 10. Visma.

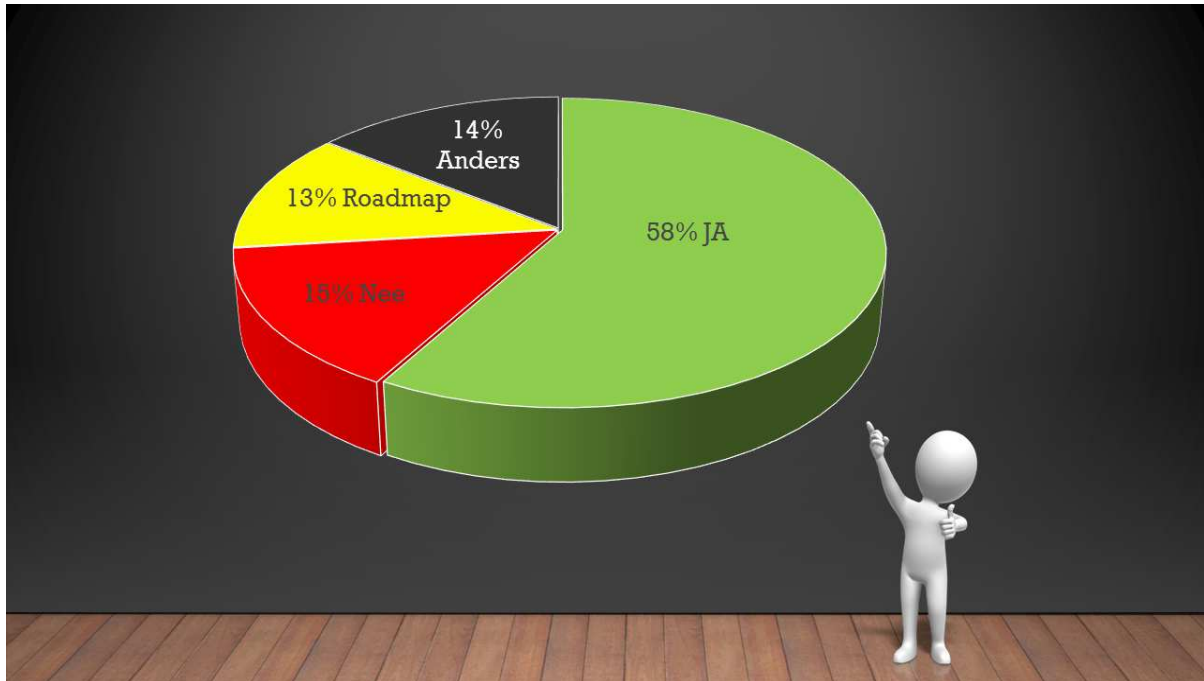
RESPONDENTEN	
1. ActiefSoftware	6. Oracle Taleo
2. Carerix	7. Otys
3. Connexys by Bullhorn	8. Talentsoft
4. Cornerstone	9. Tangram
5. HROffice	10. Visma

Indien uw leverancier niet tot bovenstaande groep van respondenten behoort, kunt u deze zelf benaderen met het verzoek de AVG-proof quickscan ATS 2018 alsnog in te vullen. Vroom Consultancy stelt de online quickscan hier zonder bijkomende kosten voor beschikbaar op https://hrmsysresearch.online/?page_id=37

Uw leverancier kan op de site een login aanvragen en het resultaat met u delen.

Globale resultaten

Hieronder ziet u het globale resultaat van de quickscan, zoals dat gepresenteerd is tijdens het webinar.



Globale resultaten AVG-proof quickscan ATS 2018

Uit bovenstaande grafiek blijkt dat:

- Meer dan de helft van de respondenten bepaalde aspecten van de AVG al ondersteunen (Ja).
- Dertien procent geeft aan een aantal zaken in ontwikkeling te hebben, zodat deze in een volgende versie van het ATS beschikbaar zijn (Roadmap).
- Vijftien procent is op onderdelen nog niet AVG-proof (Nee).
- Veertien procent biedt een alternatieve werkwijze aan of geeft een andere uitleg aan de functionaliteit zoals Vroom Consultancy die heeft vertaald vanuit het betreffende artikel uit de AVG (Anders).

Hierna volgt per vraag de gekozen antwoordopties van alle respondenten. De beantwoording per vraag per leverancier staan in de volgende hoofdstukken van dit rapport.

Resultaten per vraag

In de tabel hieronder staan de totale scores van de beantwoording per vraag. Voor de beantwoording per respondent verwijzen wij naar het hoofdstuk "Scores per leverancier".

Vraag #	Ja	Nee	Op roadmap	Anders, namelijk..
1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	100%			
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	30%		20%	50%
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	70%		30%	
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	50%	10%	10%	30%
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	50%		30%	20%
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	70%		10%	20%
7. Uw recruitment platform ondersteunt video interviews.	70%	20%	10%	
7a. Video- en ander beeldmateriaal wordt automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming gegeven voor een langere bewaartermijn.	40%	10%	30%	20%
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	70%	10%		20%

Vraag #	Ja	Nee	Op roadmap	Anders, namelijk..
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	80%	20%		
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	50%		20%	30%
11. Een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	80%	20%		
12. Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	70%	20%	10%	
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	50%	20%	20%	10%
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	60%	20%	10%	10%
14a. Van de matchingsfunctie is een DPIA-rapport beschikbaar, waarmee uw klanten ondersteund worden bij het AVG-proof werken.	10%	90%		

Conclusies en mogelijke vervolgstappen

Uit de AVG-quickscan zijn een aantal opvallende conclusies te trekken:

- Alle respondenten geven aan dat hun ATS voorziet in het op een eenvoudige en ondubbelzinnige wijze verkrijgen van toestemming voor het verwerken van persoonsgegevens voor arbeidsbemiddeling (vraag 1). Wij adviseren u om dit in de praktijk te laten valideren.
- Niet alle leveranciers ondersteunen op het moment van uitvoering van de quickscan alle functies om de rechten van de kandidaat (inzage-, correctie-, meeneemrecht en recht op vergetelheid); u zult als gebruiker van het systeem handmatige handelingen moeten verrichten om uw verplichtingen als verwerker na te komen (vragen 2, 4 en 7a).
- Het verplichte door u zelf op te leveren verwerkingsregister* wordt niet door alle leveranciers geautomatiseerd ondersteund (vraag 13). Schakel een informatiespecialist in om u hierbij te assisteren, als uw ATS hier niet in voorziet.
- De meeste leveranciers, die geautomatiseerd matchen ondersteunen, kunnen daarvoor nog geen Data Privacy Impact Assessment (DPIA)* overleggen (vraag 14a).

Meer informatie over het verwerkingsregister en het DPIA staat in de betreffende bijlage van dit rapport.

Mogelijke vervolgstappen

Als de leverancier van het ATS waar u mee werkt, niet voorkomt in de lijst met respondenten, kunt u deze benaderen met het verzoek om de, in deze quickscan gebruikte vragen, alsnog te beantwoorden. Vroom Consultancy stelt de online quickscan hier zonder bijkomende kosten voor beschikbaar op https://hrmsysresearch.online/?page_id=37

Als uw leverancier tot de groep van respondenten behoort, maar nog geen DPIA en/of geautomatiseerde ondersteuning voor het verwerkingsregister biedt, ga daar dan over in gesprek met uw leverancier.

Scores per leverancier

Hierna zijn de antwoorden op de quickscan vragen te vinden. Wij hebben deze 1 op 1 overgenomen.

Actief software

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Ja
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 2	Niet Automatisch. Overzicht van kandidaten die voldoen aan AVG eisen en met makkelijke multi selectie kan gebruiker alle geselecteerd kandidaten verwijderen
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	Ja
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 4.	Zodra definitie van " in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen" wordt duidelijker omschreven zullen wij dat implementeren. Op dit moment is zinloos om een bepaald xml formaat

	te produceren die geen enkele organisatie kan importeren.
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Op roadmap
Datum gepland 5.	28/02/2018
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Op roadmap
Datum gepland 6.	28/02/2018
7. Uw recruitment platform ondersteunt video interviews.	Nee
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in versleuteling (8).	Database server gebruikt eigen beveiliging systeem.
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Ja
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in actueel en juist houden van gegevens (10).	half-automatisch
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja

12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	Ja
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Op roadmap
Datum gepland export met gegevens voor het verwerkingsregister (13).	28/02/2018
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing matchen ondersteund ondersteund (14)	half-automatisch

Carerix

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Ja
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Ja
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	Ja
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	Ja
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Op roadmap
Datum gepland 5.	01/04/2018
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 6.	In verband met verplichtingen naar bijvoorbeeld de fiscus is het automatisch verwijderen uit het systeem een zeer ongewenste mechaniek. Bij een verwijderingsaanvraag wordt een workflow gestart om de rechtmatigheid van het verzoek te beoordelen door de DPO of andere verantwoordelijken.

	Hiermee is direct ook een workflow aan te leggen om deze gegevens eventueel uit aan palende klantsystemen te verwijderen (denk aan salarissysteem oid)
7. Uw recruitment platform ondersteunt video interviews.	Anders, namelijk..
Omschrijf kort hoe uw oplossing voorziet in functionaliteit 7.	Deze functionaliteit is geïntegreerd in Carerix maar de contractpartij is een derde partij waarmee de klant een contract afsluit. Deze partij is de verwerker van de gegevens conform GDPR
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Ja
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Ja
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Ja
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	Ja

<p>13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing het verwerkingsregister ondersteund(13).</p>	<p>partieel ondersteund, met name de kandidaat gegevens.</p>
<p>14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing matchen ondersteund ondersteund(14)</p>	<p>Carerix ondersteunt met name de processen waarin de matching een combinatie is van geautomatiseerde aspecten samen met de beoordeling van de recruiter</p>

Connexys by Bullhorn

1. Your (recruitment) solution offers a form, which allows an applicant to give permission in a simple and unequivocal manner to the processing of personal data for job placement.	Other,..
Briefly describe how your solution will support function 1.	Controllers design their form themselves or use the possibility to create a custom form (by us). The controller will be responsible for having a clear privacy notice on his form, and make sure the candidate reads it (though this is not required) before pressing the apply button.
2. Personal data will be automatically deleted 4 weeks after completing the application procedure, unless the candidate explicitly gives permission for a longer retention period.	Other,..
Briefly describe how your solution will support function 2.	The controller can by use of certain criteria determine when a candidate will be anonymised. Not all clients will use the same retention period.
3. Workflow for giving or requesting permission to retain the personal data for a longer period of time, with the purpose of candidate mediation.	Yes
4. All personal and record data can be taken to another organization if a candidate so requests.	Other,..
Briefly describe how your solution will support function 4.	Only personal data that was given by the candidate will be exported, also see Article 20 of the GDPR which states that the data subject will have the right to receive the data that he has provided.
5. Candidates can revoke their permission in the same way that they can unsubscribe to a newsletter with one mouse click.	Other,..
Briefly describe how your solution will support function 5.	No, I don't think anywhere in the GDPR this is a must. The candidate has the

	right to withdraw consent, but can also do this by contacting the recruiter.
6. All personal and record data are automatically deleted from the system when a candidate withdraws their consent.	Other,..
Briefly describe how your solution will support function 6.	If a candidate revokes his consent (through a request to the controller), the controller can then choose to delete the candidate, which will result in deletion of his candidate records, and all records linked to it. Or they can choose to anonymise the candidate records, which will result in a anonymisation of all identifiable information.
7. Your recruitment platform supports video interviews.	Yes
7a. Video and other image material will be automatically deleted, 4 weeks after termination of the application, unless the candidate explicitly consents for a longer retention period.	Other,..
Briefly describe how your solution will support function 7a.	See point 2.
8. Personal data is encrypted and stored in your recruitment solution.	Other,..
Briefly describe how your solution will support function 8.	This is an extra module which will not be delivered by default.
9. An automated process to email all candidates who have not yet given permission to process their data in in one go with a request. This preserves an important asset of the recruitment organization.	No
10. The system may automatically send an extension consent email before the 12-month period expires. This function is important to keep the candidate data up to date and correct.	Other,..

Briefly describe how your solution will support function 10.	With the anonymisation module the controller can set periods in which automatic emails could be sent for extension of the processing activity.
11. Sourcing support function: a social media plug-in that automatically translates (for example) a LinkedIn profile into a prospective candidate in the system.	No
12. Sourcing support function: A prospective candidate can be asked for permission via an automatic workflow; customizable mail templates are available for your solution.	No
13. Support processing register : An export function to a text file containing the specified elements for the processing register.	No
14. Your solution supports automated matching of candidates with vacancies.	Yes
14a. A DPIA report is available for the matching function, which supports your customers to meet GDPR-compliance.	No

Cornerstone

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 1	Ja. Het Cornerstone platform, inclusief Recruiting, is GDPR compliant. Cornerstone OnDemand heeft een gespecialiseerd Data Privacy Team, geleid vanuit Europa. In dit team zit ondermeer een Nederlandstalige Data Security Officer die kan adviseren aan de Nederlandstalige (potentiële) cliëntèle van Cornerstone OnDemand.
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 2	Ja. In Cornerstone worden persoonsgegevens van kandidaten na X-periode inactiviteit automatisch geanonimiseerd. Die periode van inactiviteit is door een organisatie zelf in te stellen. Kandidaten worden hiervan via een geautomatiseerd notificatie op de hoogte gesteld en er is een mogelijkheid voor het geven van toestemming de persoonsgegevens langer te bewaren. In verband met het kunnen blijven rapporteren op procesgegevens, worden de gegevens dus niet verwijderd, maar geanonimiseerd. Dit proces is onomkeerbaar. Cornerstone OnDemand herkent in haar wereldwijde cliëntenbestand een grote diversiteit van complexiteit en grootte. Met ondermeer cliënten in industrieën waar dataprivacy en gegevensbeveiliging van zeer groot belang zijn (zoals US Treasury, zeer veel Europese en globale banken en

	<p>financiële instituten als BNP Paribas, cliënten uit de farmaceutische industrie, (semi-)publieke organisaties en Zorginstellingen) heeft juist dit onderwerp voortdurend sterke focus en hoge prioriteit. Cornerstone OnDemand wordt onder meer gewaardeerd door cliënten en analisten voor haar strikte naleving en compatibiliteit met compliance-eisen. Cornerstone OnDemand heeft een gespecialiseerd Data Privacy Team, geleid vanuit Europa. In dit team is een Nederlandstalige Data Security Officer vertegenwoordigt die kan adviseren aan de Nederlandstalige (potentiële) cliëntèle van Cornerstone OnDemand.</p>
<p>3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 3</p>	<p>Ja. In Cornerstone worden persoonsgegevens van kandidaten na X-periode inactiviteit automatisch geanonimiseerd. Die periode van inactiviteit is door een organisatie zelf in te stellen. Kandidaten worden hiervan via een geautomatiseerde notificatie op de hoogte gesteld en er is een mogelijkheid voor het geven van toestemming de persoonsgegevens langer te bewaren. In verband met het kunnen blijven rapporteren op procesgegevens, worden de gegevens dus niet verwijderd, maar geanonimiseerd. Dit proces is onomkeerbaar.</p>
<p>4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 4.</p>	<p>Ja. Mits het voor de anonimisering van de persoonsgegevens plaatsvindt kan kandidaat informatie middels een rapport worden geëxporteerd.</p>

5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 5.	Ja, die mogelijkheid is configureerbaar door de organisatie. Deze optie zal dan verschijnen in het kandidaatportaal.
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 6.	Ja, ook deze mogelijkheid is configureerbaar door de organisatie. Deze optie zal dan tevens verschijnen in het kandidaatportaal.
7. Uw recruitment platform ondersteunt video interviews.	Ja
7a. Video- en ander beeldmateriaal wordt automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming gegeven voor een langere bewaartermijn.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 7a.	Ja. In Cornerstone worden persoonsgegevens van kandidaten na X-periode automatisch gewist. Die periode is door een organisatie zelf in te stellen. Kandidaten worden hiervan via een geautomatiseerde notificatie op de hoogte gesteld en er is een mogelijkheid voor het geven van toestemming de beeldgegevens langer te bewaren.
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in versleuteling (8).	Ja. Versleuteling (encryption at rest) is mogelijk, maar in het algemeen volgt Cornerstone al de meest stringente standaarden waar het beveiliging of privacy betreft. PII (Personal Identifiable Information) valt onder Iso-certificaat ISO/IEC27018 (Voor referentie zie ook

	https://www.cornerstoneondemand.com/company/security)
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Ja
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Ja
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	Ja
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing het verwerkingsregister ondersteund(13).	Ja, dit is mogelijk. De exporteerfunctionaliteit is algemeen beschikbaar en kan opgeslagen persoonsgegevens bevatten. Activiteitgegevens zijn geregistreerd en onderhevig aan een DPA (Data Processing Agreement) die onlosmakelijk verbonden is aan de Mantelovereenkomst tussen Cornerstone OnDemand en haar cliënten. Clienten kunnen delen van de

	DPA en/of een configureerbare "Privacy Statement" link met door de klant geformuleerde juridische bewoording toevoegen aan de voettekst van de pagina.
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing matchen ondersteund ondersteund(14)	Ja, de oplossing kan op verschillende manieren kandidaten automatisch matchen met een vacatures of functiebeschrijving. Verder is het mogelijk om van de matchingsfunctie een DPIA-rapport beschikbaar te maken, waarmee de cliëntèle van Cornerstone Ondemand ondersteund worden bij het AVG-prof werken. Cornerstone OnDemand kan haar cliënten hierbij ondersteunen, gezien zij eigenaar van de data zijn, door informatie te verstrekken in de gegevensprivacyeffectbeoordeling van haar cliënten. Cornerstone OnDemand heeft een Privacy-team dat meetbaar kan deelnemen aan het ondersteunen van klanten met beveiliging en privacybeoordelingen. Cornerstone OnDemand heeft een Nederlandstalige Data Security Officer in dienst die kan adviseren aan de Nederlandstalige (potentiële) cliëntèle van Cornerstone OnDemand.

<p>1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.</p>	<p>Ja</p>
<p>2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 2</p>	<p>via notificatie krijgt verantwoordelijke bericht dat kandidaten verwijderd dienen te worden. Verwijderen moet conform wetgeving altijd door de verantwoordelijke zelf worden gedaan. Uiteraard faciliteren wij deze mogelijkheid (1 druk op de knop)</p>
<p>3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.</p>	<p>Ja</p>
<p>4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.</p>	<p>Ja</p>
<p>5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 5.</p>	<p>kan via het contactformulier</p>
<p>6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.</p>	<p>Ja</p>

7. Uw recruitment platform ondersteunt video interviews.	Ja
7a. Video- en ander beeldmateriaal wordt automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming gegeven voor een langere bewaartermijn.	Ja
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Ja
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Ja
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in actueel en juist houden van gegevens(10).	via automatische notificatie (tijdig) waarbij de recruiter geïnformeerd wordt dat kandidaat 12 maanden in de talentpool staat en er wederom om toestemming moet worden gevraagd. De recruiter kan dan na beoordeling van de betreffende kandidaat besluiten al dan niet te willen verlengen via toestemmingsformulier
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Nee
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om	Nee

toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing het verwerkingsregister ondersteund(13).	in Verwerkersovereenkomst is vastgelegd welke gegevens wij verwerken, de contactpersonen, calamiteitenregeling (meldingsprocedure datalek), en contactgegevens functionaris gegevensbescherming. per 25 mei zal elke verwerkingsactiviteit automatisch geregistreerd worden. Via een tekstfile (log) zal deze geexporteerd kunnen worden.
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	Op roadmap

Oracle Taleo

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Ja
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Ja
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	Ja
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	Ja
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Ja
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Ja
7. Uw recruitment platform ondersteunt video interviews.	Ja
7a. Video- en ander beeldmateriaal wordt automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming gegeven voor een langere bewaartermijn.	Anders, namelijk..

Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 7a.	Hangt van partner af
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Ja
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Ja
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Ja
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	Ja
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Ja
14. Uw oplossing ondersteunt geautomatiseerd matches van kandidaten met vacatures.	Ja
14a . Van de matchingsfunctie is een DPIA-rapport beschikbaar, waarmee	Nee

uw klanten ondersteund worden bij het AVG-proof werken.	
---	--

Otys

<p>1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.</p>	<p>Ja</p>
<p>2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 2</p>	<p>Op dit moment kunnen kandidaten handmatig verwijderd worden. Op de roadmap staat dat OTYS 4 weken na beëindiging van de sollicitatieprocedure, tenzij expliciet andere toestemming is gegeven, de gegevens geanonimiseerd worden. Op deze manier kunnen plaatsingen e.d. wel meegenomen kunnen worden in rapportages.</p>
<p>3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.</p>	<p>Anders, namelijk..</p>
<p>Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 3</p>	<p>Workflows zijn op dit moment al in te stellen indien onze klanten gebruik maken van de workflow module. We werken naar een oplossing waar aan de hand van een due-date (datum waarop persoon in database terechtgekomen is) een geautomatiseerd proces start. De termijnen en e-mails in dit proces zijn uiteraard aan te passen, standaard houden we hiervoor de richtlijnen aan.</p>
<p>4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.</p>	<p>Anders, namelijk..</p>

Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 4.	Op dit moment kan een kandidaat zijn gegevens inzien bij inloggen in het kandidatenportaal. De dossiers kunnen opgevraagd worden en op dit moment op een handmatige manier verkregen worden. We werken naar de oplossing waarin de organisatie het dossier op een makkelijke wijze kan downloaden.
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Ja
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 6.	De kandidaat zal geanonimiseerd worden, net als dossier (wellicht wijken we hier nog uit naar 'wissen' of gaan we beide opties aanbieden). Afhankelijk van onze klantbehoeften.
7. Uw recruitment platform ondersteunt video interviews.	Ja
7a. Video- en ander beeldmateriaal wordt automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming gegeven voor een langere bewaartermijn.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 7a.	Indien meegenomen in het dossier (als via onze partner Clooks gaat wordt dit niet opgenomen in het dossier) zullen deze gewist en/of geanonimiseerd worden (dat laatste indien mogelijk).
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Ja
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk	Anders, namelijk..

asset van de recruitment organisatie behouden.	
Omschrijf hier kort hoe uw oplossing voorziet in het behoud van historische kandidaat-gegevens(9).	<p>Wij ondersteunen nu al een optie om een mail in een keer uit te sturen naar alle kandidaten. Ook kan er op dit moment via de beschikbaarheidsmodule al adhv mutatiegegevens geautomatiseerd mails gestuurd worden voor updaten van kandidaatgegevens. Daarna kan toestemming handmatig bijgehouden worden.</p> <p>Op de roadmap staat een oplossing om de toestemmingsknoppen (ja of nee) gelijk te koppelen aan een 'due date' waardoor een automatisch proces in werking gesteld wordt. Bij geen toestemming zal de kandidaat geanonimiseerd worden. Bij wel toestemming zal de kandidaat opgenomen worden en zullen er na 11 maanden herinneringsmails uitgaan om opnieuw om toestemming te vragen.</p>
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in actueel en juist houden van gegevens(10).	Dit kan nu adhv laatste activiteit in een kandidatendossier. Met onze AVG wijzigingen zullen we dit proces makkelijker maken en geautomatiseerd laten verlopen (adhv 'due dates')
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden;	Op roadmap

hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	
Datum gepland: email workflow voor aspirant kandidaten uit social media platforms(12).	30/04/2018
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing het verwerkingsregister ondersteund(13).	Is niet nodig. In een verwerkingsregister dienen datastromen op categorieniveau bijgehouden te worden. Deze datastromen kunnen niet geëxporteerd worden uit OTYS omdat u die zelf bepaalt. Deze categorieën en doeleinden staan wel in Annex 2 van de verwerkersovereenkomst van OTYS. Ook bieden wij op onze website een template voor een dataregister aan. Het bijhouden van dit register een een verantwoordelijkheid van de verwerkingsverantwoordelijke, niet van de verwerker.
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing matchen ondersteund ondersteund(14)	Er is een mogelijkheid voor geautomatiseerde selectie op basis van criteria. Dit proces vindt echter nooit plaats zonder menselijk handelen.

Talentsoft

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Ja
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Ja
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	Ja
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	Ja
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Ja
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Ja
7. Uw recruitment platform ondersteunt video interviews.	Nee
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Ja
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven	Ja

voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Ja
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	Ja
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Ja
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	Nee

Tangram

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Ja
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 2	Kandidaten waarvan de bewaartermijn is overschreden, worden aangeboden in een workflow. Vandaaruit kan de kandidaat worden geautomatiseerd.
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	Op roadmap
Datum gepland 3	01/07/2018
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	Anders, namelijk..
Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 4.	Oplossingsrichting vanuit de AP is nog erg onduidelijk. Dit onderwerp staat nog wel op de roadmap, realisatie gepland per 1/7
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Ja
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Anders, namelijk..

Omschrijf hier kort hoe uw oplossing voorziet in functionaliteit 6.	Niet automatisch, via workflow.
7. Uw recruitment platform ondersteunt video interviews.	Ja
7a. Video- en ander beeldmateriaal wordt automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming gegeven voor een langere bewaartermijn.	Op roadmap
Datum gepland 7a.	01/07/2018
8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Nee
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Ja
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Op roadmap
Datum gepland actueel en juist houden van gegevens(10).	01/07/2018
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden;	Ja

hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Ja
14. Uw oplossing ondersteunt geautomatiseerd matchen van kandidaten met vacatures.	Ja
14a . Van de matchingsfunctie is een DPIA-rapport beschikbaar, waarmee uw klanten ondersteund worden bij het AVG-proof werken.	Nee

1. Uw (recruitment)oplossing biedt een formulier, waarmee een aspirant kandidaat op een eenvoudige en ondubbelzinnige wijze toestemming geeft voor het verwerken van diens persoonsgegevens voor arbeidsbemiddeling.	Ja
2. Persoonsgegevens worden automatisch gewist, 4 weken na beëindiging van de sollicitatie, tenzij de kandidaat expliciet toestemming geeft voor een langere bewaartermijn.	Op roadmap
Datum gepland 2	30/04/2018
3. Workflow voor het geven of door de recruitment organisatie te vragen toestemming, om de persoonsgegevens langer te mogen bewaren met kandidaat-bemiddeling als doel.	Op roadmap
Datum gepland 3	30/04/2018
4. Alle persoons- en dossiergegevens kunnen meegenomen worden naar een andere organisatie, wanneer een kandidaat daarom vraagt.	Nee
5. Kandidaat kan diens toestemming intrekken, op dezelfde wijze waarop iemand zich met één muisklik kan uitschrijven voor een nieuwsbrief.	Op roadmap
Datum gepland 5.	30/04/2018
6. Alle persoons- en dossiergegevens worden automatisch uit het systeem verwijderd wanneer een kandidaat diens toestemming intrekt.	Ja
7. Uw recruitment platform ondersteunt video interviews.	Op roadmap
Datum gepland 7.	27/06/2018

8. Persoonsgegevens worden versleuteld opgeslagen in uw recruitment oplossing.	Ja
9. Een geautomatiseerd proces om alle kandidaten die in het verleden nog geen toestemming hebben gegeven voor verwerking van hun gegevens, in één keer te kunnen mailen met een verzoek. Hiermee blijft een belangrijk asset van de recruitment organisatie behouden.	Nee
10. Het systeem kan vóór het verstrijken van de 12 maanden toestemming, automatisch een toestemmings-mail voor verlenging sturen. Deze functie is van belang om de kandidaat-gegevens actueel en juist te houden.	Ja
11. Functie voor de ondersteuning van sourcing: een social media plug-in waarmee (bijvoorbeeld) een LinkedIn profiel automatisch wordt vertaald naar een aspirant kandidaat in het systeem.	Ja
12. Functie voor de ondersteuning van sourcing: Een aspirant kandidaat kan via een automatische workflow om toestemming gevraagd worden; hiervoor zijn aanpasbare mail templates beschikbaar uw oplossing.	Ja
13. Ondersteuning verwerkingsregister: een exportfunctie naar een tekstbestand met daarin de voorgeschreven elementen voor het verwerkingsregister.	Op roadmap
Datum gepland export met gegevens voor het verwerkingsregister(13).	30/04/2018
14. Uw oplossing ondersteunt geautomatiseerd matches van kandidaten met vacatures.	Nee

Bijlage 1 AVG-artikelen die gebruikt zijn voor de quickscan vragen.

Vraag	Vraag	Vraag	Art #	Tekst
1	2	3	Artikel 6	1. De verwerking is alleen <u>rechtmatig</u> indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
4			Artikel 20	Recht op overdraagbaarheid van gegevens 1. De betrokkene heeft het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt,...
5			Artikel 7	Voorwaarden voor toestemming Lid 3. De betrokkene heeft het recht zijn toestemming te allen tijde in te trekken. Het intrekken van de toestemming laat de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan, onverlet. Alvorens de betrokkene zijn toestemming geeft, wordt hij daarvan in kennis gesteld. Het intrekken van de toestemming is even eenvoudig als het geven ervan.
6			Artikel 17	Recht op gegevenswissing („recht op vergetelheid”) Lid1. De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen en de verwerkingsverantwoordelijke is verplicht persoonsgegevens zonder onredelijke vertraging te wissen wanneer een van de volgende gevallen van toepassing is: b) de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a), of artikel 9, lid 2, punt a), berust, in, en er is geen andere rechtsgrond voor de verwerking.

Vraag	Vraag	Vraag	Art #	Tekst
7	7a.		Artikel 4	Voor de toepassing van deze verordening wordt verstaan onder: 1) "persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); <u>als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand</u> van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer <u>elementen die kenmerkend zijn voor de fysieke</u> , fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
8			Artikel 32	Beveiliging van de verwerking 1.Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten: a) de pseudonimisering en versleuteling van persoonsgegevens;
9	10		Artikel 5	Beginselen inzake verwerking van persoonsgegevens 1. Persoonsgegevens moeten: d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid”);

Vraag	Vraag	Vraag	Art #	Tekst
11	12		Artikel 14	<p>Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen 1. Wanneer persoonsgegevens niet van de betrokkene zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie:</p> <p>a) de identiteit en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke;</p> <p>b) in voorkomend geval, de contactgegevens van de functionaris voor gegevensbescherming;</p> <p>c) de verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd, en de rechtsgrond voor de verwerking; d) de betrokken categorieën van persoonsgegevens;</p> <p>e) in voorkomend geval, de ontvangers of categorieën van ontvangers van de persoonsgegevens;</p> <p>f) in voorkomend geval, dat de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een ontvanger in een derde land of aan een internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of, in het geval van de in artikel 46, artikel 47 of artikel 49, lid 1, tweede alinea, bedoelde doorgiften, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd.</p> <p>2. Naast de in lid 1 bedoelde informatie verstrekt de verwerkingsverantwoordelijke de betrokkene de volgende informatie om ten overstaan van de betrokkene een behoorlijke en transparante verwerking te waarborgen:</p> <p>a) de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;</p> <p>b) de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, indien de verwerking op artikel 6, lid 1, punt f), is gebaseerd;</p> <p>c) dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om inzage van en rectificatie of wissing van persoonsgegevens of</p>

Vraag	Vraag	Vraag	Art #	Tekst
				<p>om beperking van de hem betreffende verwerking, alsmede het recht tegen verwerking van bezwaar te maken en het recht op gegevensoverdraagbaarheid;</p> <p>d) wanneer verwerking op artikel 6, lid 1, punt a) of artikel 9, lid 2, punt a), is gebaseerd, dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking daarvan;</p> <p>e) dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;</p> <p>f) de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen;</p> <p>g) het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.</p> <p>3. De verwerkingsverantwoordelijke verstrekt de in de leden 1 en 2 bedoelde informatie:</p> <p>a) binnen een redelijke termijn, maar uiterlijk binnen één maand na de verkrijging van de persoonsgegevens, afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt;</p> <p>b) indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene; of</p> <p>c) indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.</p> <p>4. Wanneer de verwerkingsverantwoordelijke voornemens is de persoonsgegevens verder te verwerken voor een ander doel dan dat waarvoor de persoonsgegevens zijn verkregen, verstrekt de verwerkingsverantwoordelijke de betrokkene vóór die verdere verwerking informatie over dat andere doel en alle relevante verdere informatie als bedoeld in lid 2.</p>

Vraag	Vraag	Vraag	Art #	Tekst
				<p>5. De leden 1 tot en met 4 zijn niet van toepassing wanneer en voor zover:</p> <p>a) de betrokkene reeds over de informatie beschikt;</p> <p>b) het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen, in het bijzonder bij verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, behoudens de in artikel 89, lid 1, bedoelde voorwaarden en waarborgen, of voor zover de in lid 1 van dit artikel bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. In dergelijke gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten, de vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van de informatie;</p> <p>c) het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of lid statelijk recht dat op de verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen; of</p> <p>d) de persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of lid statelijke recht, waaronder een statutaire geheimhoudingsplicht.</p>

Vraag	Vraag	Vraag	Art #	Tekst
13			Artikel 30	<p>1. Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:</p> <p>a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming; ,</p> <p>b) de verwerkingsdoeleinden;</p> <p>c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;</p> <p>d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties; ,</p> <p>e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen; ,</p> <p>f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;</p> <p>g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.</p>
14	14a		Artikel 22	<p>1. De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.</p>

Vraag	Vraag	Vraag	Art #	Tekst
			Artikel 35	Gegevensbeschermingseffectbeoordeling Lid 3. Een gegevensbeschermingseffectbeoordeling (DPIA) als bedoeld in lid 1 is met name vereist in de volgende gevallen: a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

Bijlage 2 Verwerkingsregister en DPIA

Verwerkingsregister

Hieronder citeren wij het AVG-artikel over het verwerkingsregister. Dit register zult u zelf aan moeten leggen en moeten bijhouden.

Artikel 30 "Register van de verwerkingsactiviteiten"

1. Elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een register van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:

- a) de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
- b) de verwerkingsdoeleinden;
- c) een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- d) de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- e) indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49, lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
- f) indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- g) indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

DPIA

Hieronder citeren wij het relevante deel van het AVG-artikel over de gegevensbeschermingseffectbeoordeling, in Engels het Data Privacy Impact Assessment of DPIA. Een DPIA is op termijn verplicht en dient door de leverancier van uw ATS uitgevoerd te worden. Vraag er actief naar, want u bent als verwerker verantwoordelijk

Artikel 35 Gegevensbeschermingseffectbeoordeling

Lid 3. Een gegevensbeschermingseffectbeoordeling (DPIA) als bedoeld in lid 1 is met name vereist in de volgende gevallen:

a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen.

Hieronder citeren wij een deel van de informatie over het DPIA zoals dat staat op de site van de Autoriteit Persoonsgegevens.

“De verplichting om een *data protection impact assessment* (DPIA) te doen geldt in principe alleen voor nieuwe verwerkingen. Dus voor verwerkingen die ná 25 mei 2018 starten. Vanaf die datum is de Algemene verordening gegevensbescherming (AVG) van toepassing. Treedt er na 25 mei 2018 een verandering op in een bestaande verwerking of in de risico’s van die verwerking? Dan kan een DPIA alsnog verplicht zijn.

Veranderingen bestaande verwerkingen

Een bestaande gegevensverwerking kan bijvoorbeeld veranderen **als u een nieuwe technologie gaat gebruiken**. Of als u de persoonsgegevens voor een ander doel gaat gebruiken.

In die situaties moet u, net als bij een nieuwe gegevensverwerking, vaststellen of de gewijzigde verwerking waarschijnlijk een hoog privacy risico oplevert. Zo ja, dan bent u alsnog verplicht een DPIA uit te voeren.”

Kijk voor meer informatie op:

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia>

Bijlage 3 Nuttige links

Hieronder een aantal nuttige links over de AVG en hoe zich hierop moet voorbereiden.

- <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg>
- <https://rvo.regelhulpenvoorbedrijven.nl/avg/welkom>
- werf-en.nl/avg-recruitmentbranche-compleet-overzicht/
- www.privacy-regulation.eu/nl/index.htm/

Disclaimer

Dit rapport geeft geen juridische adviezen en er kunnen op geen enkele wijze rechten aan de inhoud ontleend worden.

Vroom Consultancy heeft dit rapport met zorg samengesteld. Onjuistheden kunnen onbedoeld voorkomen. Vroom Consultancy is op geen enkele wijze aansprakelijk, noch kan zij verantwoordelijk worden gehouden voor welke geleden schade dan ook welke voortvloeit uit de door de in dit rapport verstrekte informatie.

Hieronder valt onder meer, maar niet uitsluitend, het inbreuk plegen op auteursrechtelijk beschermde werk(en) of het anderszins in strijd handelen met de intellectuele eigendomsrechten van derden.

Over de auteurs



Nienke Meindersma is senior consultant, heeft in het verleden gewerkt als Recruiter en HCM-consultant. Zij is door die ervaring gespecialiseerd in selectie en implementatie van standalone Applicant Tracking Systemen en HR-systemen mét geavanceerde ATS-functionaliteiten.



Howard Woei is management consultant, projectleider en bovenal als onafhankelijk HR-adviseur bij selectie, implementatie of optimalisatie van HR-processen en -systemen in het algemeen.