



## Werken volgens de GDPR (AVG) richtlijnen

Wat is de impact van de Algemene Verordening Gegevensbescherming (AVG) op uw recruitmentproces en organisatie en hoe ondersteunt Tangram u hierbij?

### Auteur:

Edwin Adams – Tangram

Maart 2018

## Inleiding

Op 25 mei 2018 is een nieuwe Europese privacywet in werking getreden: de Algemene Verordening Gegevensbescherming (AVG). Deze verordening is internationaal ook wel bekend onder de naam General Data Protection Regulation (GDPR).

Deze regelgeving zal in alle lokale privacywetten binnen de hele EU en Europese Economische Ruimte (EER) worden geïmplementeerd. De verordening geldt voor alle organisaties die producten of diensten verkopen aan burgers in Europa en hun persoonsgegevens verwerken, inclusief bedrijven op andere continenten. De verordening biedt burgers in de EU en EER meer controle over hun persoonsgegevens en moet waarborgen dat hun informatie in heel Europa goed wordt beschermd.

De nieuwe AVG vervangt de gegevensbeschermingsrichtlijn 95/46/EG. De AVG is rechtstreeks van toepassing in elke lidstaat en zal leiden tot een betere harmonisatie van gegevensbescherming tussen de EU-landen.

Hoewel veel bedrijven inmiddels al eigen privacyprocessen en -procedures hebben vastgesteld in overeenstemming met de richtlijn, bevat de AVG een aantal nieuwe waarborgen voor EU-Burgers van wie gegevens worden verzameld. Zodra de AVG van kracht is, dreigen er forse boetes en straffen voor gegevensverantwoordelijken en verwerkers die zich niet aan de regels houden.

De AVG maakt het noodzakelijk dat bedrijven die persoonsgegevens van EU-Burgers verwerken hun verwerkingsproces zodanig aanpassen, dat deze in lijn is met de nieuwe Verordening.

In deze whitepaper leest u hoe u met inzet van Tangram software werkt conform de nieuwe wetgeving. Dit document vervangt de eerder uitgebrachte versie (augustus 2017).

## De GDPR in het kort

- De GDPR is in werking getreden op 27 april 2016 en gepubliceerd in Pb EU L119 d.d. 4 mei 2016
- Deze vervangt de Europese privacyrichtlijn 95/46/EC van 24 oktober 1995
- De GDPR is van toepassing vanaf 25 mei 2018. Van organisaties wordt verwacht dat zij de bedrijfsvoering in overeenstemming brengen met de GDPR. Na 25 mei 2018 wordt naleving gecontroleerd door de Autoriteit Persoonsgegevens (AP).

Het effect van de GDPR is ook dat de bevoegdheden voor alle Europese privacy toezichthouders gelijk worden getrokken. Organisaties krijgen slechts met één Data Protection Authority (DPA) te maken. De nationale DPA's, zoals in Nederland de Autoriteit

Persoonsgegevens (AP), worden dan door één European Data Protection Board (EDPB) gecoördineerd.

Hieronder volgt een toelichting van de belangrijkste begrippen en wat de impact is van de GDPR/AVG voor organisaties die de software van Tangram gebruiken.

### **Hoe ondersteunt Tangram u bij het werken conform de nieuwe richtlijnen?**

Niet alle richtlijnen uit de GDPR hebben betrekking op de software van Tangram. U dient zelf ook een aantal organisatorische maatregelen te nemen. Zorg ervoor dat de relevante mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. [Stappenplannen zoals op de website van de Autoriteit Persoonsgegevens](#) zijn hierbij een handig hulpmiddel.

Tevens is er een handige [online checklist](#), waarmee u stap voor stap kunt bepalen hoe ver uw organisatie is met de invoering van de AVG.

## Gerechtvaardigd Doel en Grondslag van de verwerking

In het kader van werving & selectie of (interne) mobiliteit heeft u een gerechtvaardigd doel om gegevens te verwerken. U zult ook één of meerdere grondslagen moeten hebben waarop u de gegevens mag verwerken.

### Grondslag verwerking persoonsgegevens

Een belangrijk aspect van de AVG is dat u een wettelijk grondslag moet hebben om persoonsgegevens te verwerken. **Let op:** voor het verwerken van bijzondere persoonsgegevens als godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele voorkeur, lidmaatschap van een vakbond, strafrechtelijk verleden of het burgerservicenummer (BSN) gelden wettelijke eisen. Een organisatie mag geen bijzondere persoonsgegevens gebruiken, tenzij daarvoor in de wet een uitzondering is. Zie daarvoor de **grondslag verwerking bijzondere persoonsgegevens** verderop in dit document.

U kunt zich baseren op één of meerdere van de volgende grondslagen voor het verwerken van persoonsgegevens:

#### 1. Toestemming van de betrokken persoon.

De AVG schrijft niet precies voor in welke vorm u toestemming moet vragen. Maar de manier waarop u toestemming vraagt moet wel voldoen aan een aantal specifieke eisen.

Rechtsgeldige toestemming voldoet aan de volgende eisen:

- Vrijelijk gegeven: u mag iemand niet onder druk zetten om toestemming te geven. Bijvoorbeeld door iemand te benadelen als hij of zij geen toestemming geeft. Let daarbij op machtsverhoudingen: een werknemer kan een vraag van zijn werkgever bijvoorbeeld moeilijk weigeren.
- Ondubbelzinnig: er moet sprake zijn van een duidelijke actieve handeling. Bijvoorbeeld een (digitale) schriftelijke of een mondelinge verklaring. Het moet in elk geval volstrekt helder zijn dát er toestemming is verleend. U mag niet uit gaan van het principe 'wie zwijgt, stemt toe'. Het gebruik van vooraf aangevinkte vakjes is dus niet toegestaan.
- Geïnformeerd: u moet mensen informeren over:
  - de identiteit van uw organisatie;
  - het doel van elke verwerking waarvoor u toestemming vraagt;
  - welke persoonsgegevens u verzamelt en gebruikt;
  - het recht dat zij hebben om de toestemming weer in te trekken.

Informatie dient u in een toegankelijke vorm aan te bieden. Ook moet deze begrijpelijk zijn zodat iemand een weloverwogen keuze kan maken. Dat betekent dat u duidelijke en eenvoudige taal moet gebruiken.

- Specifiek: toestemming moet steeds gelden voor een specifieke verwerking en een specifiek doel. Indien u als organisatie bij de verwerking meerdere doeleinden heeft, dient u de betrokkene hierover te informeren en betrokkene voor elk doel afzonderlijk toestemming te vragen. Het doel mag niet gaandeweg veranderen.
- Het moet voor mensen net zo makkelijk zijn de toestemming weer in te trekken als dat het was om de toestemming te geven.
- Een verkregen geldige toestemming dient u aan te kunnen tonen indien de Autoriteit Persoonsgegevens daarom vraagt.

Voldoet de toestemming niet aan deze eisen? Dan is de toestemming niet geldig. De persoonsgegevens mogen dan niet verwerkt worden.

Binnen recruitmentprocessen is het gebruikelijk toestemming te vragen voor het verstrekken van sollicitatiegegevens. Tangram ondersteunt dit op de volgende aspecten:

1. Bij het indienen van een sollicitatie op het Tangram Internet Service platform (TIS) dient de kandidaat akkoord te gaan met de voorwaarden zoals gesteld in de 'disclaimer'. Met deze disclaimer voldoet u aan het aspect 'geïnformeerd' en hierin kan ook een verwijzing worden opgenomen naar de voorwaarden in uw privacy statement op uw eigen website. Meer details over de **privacy statement** is verderop in dit document weergegeven.
2. Een tweede (apart opgestelde) disclaimer is van toepassing als de kandidaat een gebruikersaccount aanmaakt op TIS om hiermee het sollicitatiedossier te onderhouden. Niet elke klantomgeving biedt de mogelijkheid dit te doen. Deze disclaimer kan afwijkend zijn omdat het hier gaat om een sollicitatiedossier dat de kandidaat zelf kan onderhouden. De standaard bewaartermijn hiervoor is 1 jaar na de laatste inlogsessie van de kandidaat.
3. Voor de eveneens optionele keuze van de vacature e-mailservice op TIS kan een derde (apart opgestelde) disclaimer worden ingesteld. Met het instellen van de e-mailservice legt u alleen een e-mailadres van de kandidaat vast. Op korte termijn wordt bij de vacature e-mailservice een functionaliteit toegevoegd zodat elk jaar gevraagd wordt of de kandidaat het abonnement op de service wil verlengen. Deze gegevens zijn voor u als verantwoordelijke niet inzichtelijk, maar Tangram is de verwerker van deze gegevens namens u, de verantwoordelijke. Zie ook het onderwerp **Verwerkersovereenkomst** verderop in het document.

4. Naast dat de kandidaat een bewuste keuze maakt om akkoord te gaan met de voorwaarden, kan deze ook een keuze maken voor de termijn dat de sollicitatiegegevens gebruikt mogen worden. Is dit alleen voor de specifieke vacature (Tangram ondersteunt de richtlijn vanuit de AP om een termijn van vier weken na afronding van de procedure te gebruiken) of ook voor mogelijke toekomstige functies (met als maximale termijn één jaar). Indien u over een maatwerkapplicatie beschikt, heeft u de mogelijkheid hiervan af te wijken. Zie ook de uitleg over **bewaartermijnen** verderop in dit document.
5. Indien de kandidaat gebruik maakt van een gebruikersaccount, kan deze de toestemming op elk moment ook weer intrekken. Datzelfde geldt voor de vacature e-mailservice.
6. In de Tangram software wordt vanaf release 2017.2 vastgelegd wanneer de toestemming is verkregen en, indien u als klant met een maatwerkapplicatie hiervoor gekozen heeft, voor welke termijn u de gegevens van de kandidaat mag verwerken. Vanaf release 2018.1 wordt ook vastgelegd vanaf welk IP-adres dit is gebeurd. Mocht het zover komen dat u aan de Autoriteit Persoonsgegevens moet aantonen dat u de toestemming van de kandidaat heeft verkregen, dan zijn deze gegevens nodig. Dit is overigens alleen van toepassing op nieuwe sollicitaties die via het TIS platform zijn gedaan. Indien u op een andere wijze sollicitaties verwerkt (of kandidaten aanmaakt), zult u de toestemming zelf moeten vastleggen.

## 2. De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.

Deze grondslag is van toepassing zodra u een overeenkomst heeft met iemand en hiervoor het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens, maar dient een ander doel te hebben.

Let op dat u geen persoonsgegevens verwerkt die niet noodzakelijk zijn voor de uitvoering van de overeenkomst. Doet u dat wel, dan moet u rechtsgeldige toestemming of een andere grondslag hebben om deze gegevens te mogen verwerken.

Zijn de persoonsgegevens echt noodzakelijk voor de naleving van de overeenkomst met ieder betrokken individu? Om u op deze grondslag te baseren, is een goede onderbouwing nodig. Onder de AVG heeft u namelijk een verantwoordingsplicht. Zie hiervoor ook het onderwerp **Verwerkingsregister**.

### **3. De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.**

Wilt u zich op deze grondslag baseren? Dan moet de verwerking van de persoonsgegevens noodzakelijk zijn om aan een wettelijke verplichting te voldoen. Bijvoorbeeld: u heeft een bevel van de politie om bepaalde persoonsgegevens aan hen te verstrekken. Of: u verstrekt gegevens voor de uitvoering van de belastingwet.

Het hoeft niet expliciet in de wet te staan dat u voor de uitvoering van een specifieke taak persoonsgegevens moet verwerken. Soms is de verplichting in de wet namelijk ruimer geformuleerd. Het is dan aan u te bepalen of het verwerken van persoonsgegevens noodzakelijk is om aan uw verplichting te voldoen.

In de Tangram software is het mogelijk gegevens vast te leggen die betrekking hebben op de arbeidsrelatie. In dat geval heeft u een (toekomstige) overeenkomst tussen u en de kandidaat of kunt u zich beroepen op het nakomen van een wettelijke verplichting. Denk daarbij aan de registratie van trajecten in het kader van bijvoorbeeld re-integratie, outplacement of reorganisatie. U kunt zelf het beste inschatten of deze situatie voor u van toepassing is.

### **4. De gegevensverwerking is noodzakelijk voor behartiging van de gerechtvaardigde belangen.**

De gegevensverwerking kunt u op deze grondslag baseren als u aan drie voorwaarden voldoet: (1) u heeft een gerechtvaardigd belang, (2) de verwerking is noodzakelijk om dit gerechtvaardigde belang te behartigen en (3) u heeft een afweging gemaakt tussen uw belangen en die van de personen van wie u persoonsgegevens verwerkt.

1. Gerechtvaardigd belang: Het gerechtvaardigd belang moet rechtmatig, voldoende duidelijk verwoord en ook echt aanwezig zijn. Dit is van toepassing zodra een verwerking aantoonbaar noodzakelijk is om uw bedrijfsactiviteiten te verrichten. Bijvoorbeeld het voeren van een personeelsadministratie.
2. Noodzakelijkheid: De verwerking van de persoonsgegevens moet noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang. Daarom dient u de verwerking te toetsen aan de eisen van: (1) proportionaliteit en (2) subsidiariteit. Dat betekent dat u moet nagaan of (1) het doel van de verwerking in verhouding staat tot de inbreuk voor de personen van wie u persoonsgegevens verwerkt en (2) of u het doel niet op een voor de betrokken personen minder nadelige manier kunt bereiken.

3. Afweging belangen: U moet een afweging maken tussen uw belangen en de belangen van de personen van wie u persoonsgegevens verwerkt. Ook moet u hierbij eventueel maatregelen treffen om ervoor te zorgen dat de rechten en vrijheden van deze personen niet zwaarder wegen dan uw gerechtvaardigd belang.

Voorbeeld: deze grondslag kunt u toepassen indien u een kandidaat vindt in LinkedIn. In dat geval mag u de kandidaat voor een beperkte periode (dertig dagen) zonder toestemming opslaan in uw database. Vervolgens dient u eerst de kandidaat te benaderen met de vraag of u specifieke informatie mag opsturen, waarbij u direct aangeeft wat uw beleid is ten aanzien van het verwerken van gegevens en welke bewaartermijn u hanteert. Het antwoord dat u per mail terugkrijgt, slaat u op als contact in de Tangram software. Daarna kunt u pas de specifieke vacature informatie versturen. Indien u geen toestemming krijgt voor het versturen van deze informatie, markeert u de kandidaat weer om deze te verwijderen. Zie hiervoor de toelichting bij het onderwerp **Bewaartermijn** verderop.

5. **De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.**
6. **De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.**

Het ligt niet voor de hand dat u de Tangram software inzet voor doeleinden waarbij u zich kunt beroepen op één van deze grondslagen, dus deze worden niet verder uitgediept in deze whitepaper. Indien u hier meer informatie over wilt, kunt u terecht op de [website](#) van de Autoriteit Persoonsgegevens.

### **Grondslag verwerking bijzondere persoonsgegevens**

Zoals eerder aangegeven is de verwerking van bijzondere persoonsgegevens verboden, tenzij u zich kunt beroepen op een wettelijke uitzondering én op één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens. In de praktijk vallen sommige van die grondslagen samen.

In de AVG staan tien uitzonderingen op het verbod bijzondere persoonsgegevens te verwerken. Dat betekent dat het verbod niet voor u geldt zodra u zich kunt beroepen op één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens én indien:

1. Iemand uitdrukkelijk toestemming heeft gegeven voor de verwerking van zijn/haar persoonsgegevens.
2. De verwerking noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van u of de betrokken persoon, bijvoorbeeld



op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht.

3. De verwerking noodzakelijk is ter bescherming van de vitale belangen van de betrokken persoon of van een andere natuurlijke persoon. Dit geldt alleen wanneer diegene fysiek of juridisch niet in staat is om zijn toestemming te geven.
4. De verwerking wordt gedaan door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is, die die gegevens verwerkt in het kader van gerechtvaardigde activiteiten en met passende waarborgen.
5. De verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.
6. De verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Of wanneer partijen handelen in het kader van hun rechtsbevoegdheid.
7. De verwerking noodzakelijk is vanwege een zwaarwegend algemeen belang.
8. De verwerking noodzakelijk is voor doeleinden van preventieve of (arbeids)geneeskundige aard. Zoals het beoordelen van arbeidsgeschiktheid en/of het verstrekken van gezondheidszorg.
9. De verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid.
10. De verwerking noodzakelijk is met het oog op de archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

U dient alert te zijn op het vastleggen van BSN, identificatienummer, kopie ID-bewijs, bankrekening en medische gegevens. Vervolgens dient u goed te kijken welke gegevens bijvoorbeeld in een re-integratie traject worden vastgelegd en welke personen toegang hebben tot deze informatie. Dit zijn bijzondere persoonsgegevens, dus u dient zelf een afweging te maken of het registreren van deze gegevens in de Tangram software past binnen het kader van uw verwerkingsgrondslag.

## Verplichtingen vanuit de AVG

Onder de AVG hebben organisaties een stevige informatieplicht. Dat betekent dat u personen van wie u gegevens wilt verwerken duidelijk moet informeren over wat u met hun persoonsgegevens gaat doen. Het betekent ook dat u gegevens moet kunnen overleggen aan de Autoriteit Persoonsgegevens als deze daarom vraagt.

### Privacy statement

U kunt via een online privacy statement gebruikers informeren over wat u met hun persoonsgegevens gaat doen. Vanuit een sollicitatieformulier op TIS of in een e-mail kunt u een verwijzing maken naar dit statement, zodat deze eenvoudig te raadplegen is.

Het privacy statement mag volgens de AVG niet te lang en niet ingewikkeld zijn. Het moet voor gebruikers makkelijk te begrijpen zijn wat u als organisatie met de persoonsgegevens doet. Daarom dient u onder meer te laten weten:

- Wie u bent (bedrijfsnaam en contactgegevens). Indien u een functionaris gegevensbescherming heeft, dient u deze contactgegevens ook te vermelden. Zie onderdeel **functionaris gegevensbescherming**.
- Welke persoonsgegevens u verwerkt. Zie onderdeel **verwerkingsregister**.
- Voor welk specifieke doel en welke grondslag u de gegevens verwerkt. Indien u de grondslag '**uitvoering van een overeenkomst**' of '**nakomen van een wettelijke verplichting**' gebruikt, dient u ook aan te geven wat de gevolgen zijn van het niet verstrekken van de persoonsgegevens. Indien de grondslag '**toestemming**' is, dient u aan te geven dat de toestemming ook weer ingetrokken mag worden.
- Wat de duur is van de opslag (welke criteria bepalen hoe lang gegevens worden opgeslagen). Zie onderdeel **bewaartermijn**.
- Dat de betrokkene recht heeft op inzage, rectificatie en het laten verwijderen van persoonsgegevens. Hierbij kunt u ook aangeven hoe de betrokkene dit recht kan uitoefenen. Zie onderdeel **rechten en plichten**.
- Dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens.
- Aan welke categorieën van ontvangers de persoonlijke gegevens worden doorgegeven. Dat zijn bijvoorbeeld (potentiële) werkgevers, maar ook Tangram als verwerker van gegevens namens u als verantwoordelijke.
- Indien er sprake is van geautomatiseerde besluitvorming of profilering, dient u te vermelden waarom dit gedaan wordt en wat de verwachte gevolgen daarvan zijn.

Heeft u al wel een privacy statement op uw website, maar heeft u op het TIS sollicitatieformulier nog geen verwijzing hiernaar? Geef dit dan door aan onze helpdesk, zodat wij dit voor u in orde kunnen maken.

### **Functionaris Gegevensbescherming/Data Protection Officer**

Bedrijven kunnen verplicht worden gesteld een Functionaris Gegevensbescherming (FG) of Data Protection Officer aan te stellen. Vooralsnog geldt dit alleen voor organisaties waarvoor dataverwerking het primaire proces is. Zo'n functionaris was in de Wbp niet verplicht, maar is het onder de AVG in sommige situaties wel. De FG is een persoon die toeziet op de omgang met persoonsgegevens binnen een organisatie. Ook controleert deze of de organisatie voldoet aan de wet en toepasselijke regelgeving. Of uw organisatie de verplichting heeft om een FG aan te stellen, kunt u nagaan op de [website](#) van de Autoriteit Persoonsgegevens.

### **Verwerkingsregister**

De AVG legt meer verantwoordelijkheid bij u als organisatie om aan te tonen dat u aan de privacyregels voldoet. Door te voldoen aan uw verantwoordingsplicht (accountability) levert u een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

De nieuwe regels dwingen u goed na te denken over de wijze waarop uw organisatie persoonsgegevens verwerkt en beschermt. De verantwoordingsplicht houdt in dat u moet kunnen aantonen dat uw verwerkingen aan de regels van de AVG voldoen. Daarom dient u bijvoorbeeld aan te tonen dat een verwerking aan de belangrijkste beginselen van de verwerking voldoet, zoals rechtmatigheid, transparantie, doelbinding en juistheid. Ook dient u te laten zien dat u de juiste technische en organisatorische maatregelen hebt genomen om de persoonsgegevens te beschermen. Tot slot moet u kunnen laten zien dat u gebruikers (kandidaten) goed heeft geïnformeerd over de verwerking van hun persoonsgegevens. U kunt hiervoor uw privacyverklaring gebruiken.

Organisaties met meer dan 250 medewerkers zijn verplicht een register bij te houden. Ook als u minder dan 250 werknemers heeft, maar u zich structureel (niet-incidenteel) bezighoudt met het verwerken van persoonsgegevens (al dan niet in de categorie bijzondere persoonsgegevens), dan moet u dit register kunnen verstrekken wanneer de Autoriteit Persoonsgegevens daar om vraagt. Kortom, alle klanten van Tangram (een enkele uitzondering daargelaten) moeten een dataregister opstellen.

De AVG schrijft niet voor in welke vorm u dit verwerkingsregister dient bij te houden, maar deze dient minimaal een aantal onderdelen te bevatten, waarvan hieronder een opsomming staat. Een flink aantal elementen dient overeen te komen met de inhoud van

## Werken volgens de GDPR (AVG) richtlijnen

---

de privacy statement. Tangram adviseert u echter hiervoor een aparte registratie te maken. Overigens heeft dit register niet alleen betrekking op de software van Tangram. Hierbij dient u ook andere systemen en processen te betrekken, bijvoorbeeld HRM systemen (salaris en verzuim), CRM systeem etc.

- De naam en contactgegevens van uw organisatie, of de vertegenwoordiger van uw organisatie.
- Eventuele andere organisaties met wie u gezamenlijk de doelen en middelen van de verwerking heeft vastgesteld.
- De functionaris voor de gegevensbescherming, mits u die heeft aangesteld.
- Eventuele andere internationale organisaties waar u persoonsgegevens mee deelt.
- De doelen waarvoor u de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bemiddelen van personeel of het uitvoeren van direct marketing (vacature e-mailservice).
- Een beschrijving van de categorieën van personen van wie u gegevens verwerkt zoals bijvoorbeeld klanten en kandidaten.
- Een beschrijving van de categorieën van persoonsgegevens (let op, onderstaande opsomming hoeft voor u nog niet uitputtend te zijn):
  - NAW gegevens
  - Identificatiegegevens
  - Sociale media profielen
  - Persoonlijke kenmerken
  - Opleiding en vorming
  - Beroep en betrekking
  - Burgerservicenummer
  - Website gedrag (IP-nummer)
- Welke wettelijke grondslag u gebruikt:
  - Toestemming
  - Contractuele overeenkomst
  - Wettelijke verplichting
  - Vitaal belang
  - Taak van algemeen belang
  - Gerechtvaardigd belang
- De datum waarop u de gegevens moet wissen (als dat bekend is). Zie hiervoor het onderdeel **bewaartermijn**.
- De categorieën van ontvangers aan wie u persoonsgegevens verstrekt.
- Deelt u de gegevens met een land of internationale organisatie buiten de EU? Dan dient u dit aan te geven in het register.
- Een algemene beschrijving van de technische en organisatorische maatregelen die u heeft genomen om persoonsgegevens die u heeft verwerkt te beveiligen.

Volgens de GDPR (AVG) richtlijnen dient u zelf dit register te onderhouden en aan te passen aan een nieuwe situatie, mocht zich dat voordoen.

### **Verwerkersovereenkomst**

Met de komst van GDPR (AVG) wordt een duidelijkere scheiding aangebracht tussen de verantwoordelijkheid van de data-eigenaar (verantwoordelijke) en die van de data-verwerker (verwerker). Als organisatie bent u de data-eigenaar van de persoonsgegevens. Tangram als organisatie verwerkt, in opdracht van u als verantwoordelijke, persoonsgegevens bij het gebruik van bepaalde diensten. Denk hierbij aan de Tangram Internet Service diensten ('werkenbij-site', sollicitatieformulier), TIS Manager/Online Dashboard, Cloud Database en Microsoft Dynamics/CRMatch. Daarnaast kan het zijn dat Tangram op haar beurt ook derden inschakelt bij de verwerking van persoonsgegevens. Denk hierbij aan de CV extractie van Textkernel, video-solliciteren met Flipbase en de hostingpartij die de infrastructuur beheert.

**TIP:** Mocht u nog geen verwerkersovereenkomst met Tangram hebben afgesloten, dan kunt u contact opnemen onze helpdesk. Vervolgens sturen wij u een verwerkersovereenkomst.

### **Verantwoordingsplicht toestemming**

Naast een verwerkersregister en een verwerkersovereenkomst dient u bij de grondslag 'Toestemming' aan de Autoriteit Persoonsgegevens te kunnen laten zien dat u deze toestemming daadwerkelijk heeft. Dat maakt onderdeel uit van de verantwoordingsplicht die u onder de GDPR (AVG) heeft.

Twee van de eisen die de AVG stelt aan 'toestemming' zijn dat deze 'geïnformeerd' en 'specifiek' gegeven is. Om een geldige toestemming aan te tonen is het dan ook essentieel dat u kunt laten zien op basis van welke informatie de betrokken personen de toestemming hebben gegeven. Deze informatie kunt u combineren met documentatie over het proces waarin u heeft vastgelegd op welke manier u toestemming ontvangt en vastlegt.

In release 2017.2 is de eerste stap gezet om bij een kandidaat ook de datum vast te leggen zodra deze toestemming heeft gegeven (of heeft ingetrokken) en voor welke termijn dit van toepassing is. Dit geldt specifiek voor klanten met een standaardversie ("Compact") en klanten met een maatwerkversie ("Power") die hebben gekozen voor het optionele pakket GDPR Extra. In release 2018.1 is het ook mogelijk geworden om vast te leggen via welk IP-nummer de toestemming is gegeven.

Naast het vastleggen van deze toestemming krijgt u met de 2018.1 update ook de mogelijkheid om kandidaten, waarvan de toestemming op korte termijn verloopt of kandidaten waarbij u nog geen toestemming heeft vastgelegd een e-mail te sturen. In deze e-mail wordt de vraag gesteld of de kandidaat de toestemming wil verlengen of intrekken. Het antwoord wordt automatisch in de Tangram software verwerkt. Uiteraard wordt ook workflow aangeboden om dit proces eenvoudig te kunnen beheren.

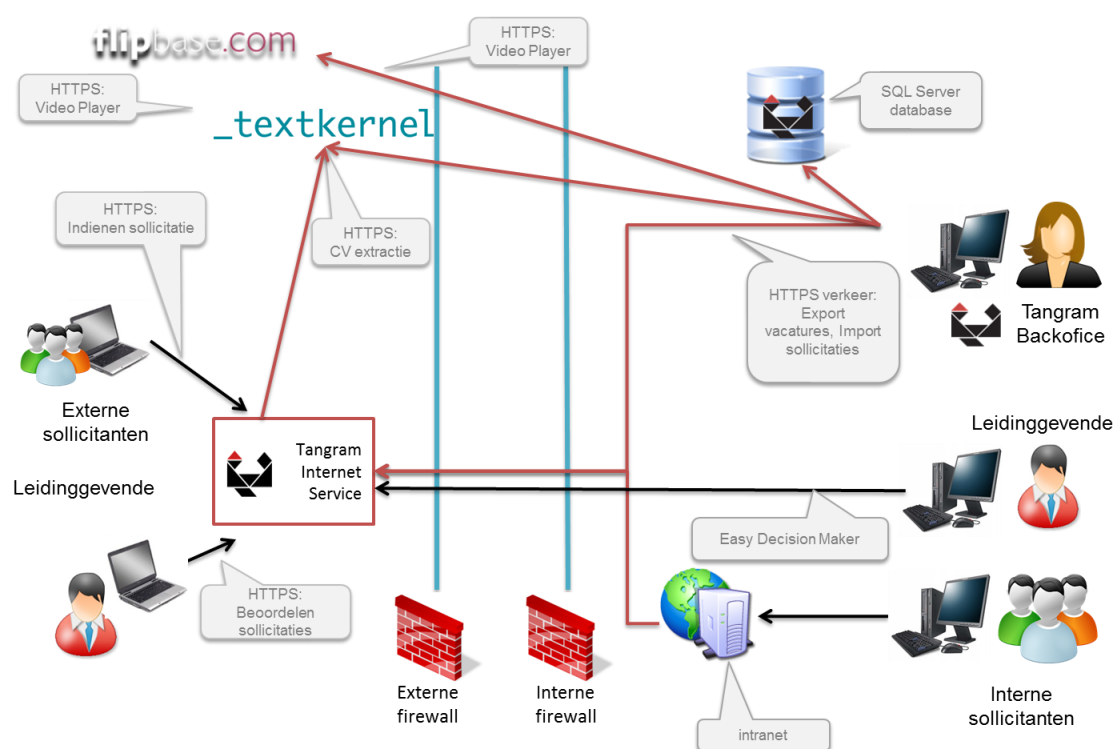
Bij de automatische verwerking van de reactie van de kandidaat wordt het IP-nummer vastgelegd, zodat u kunt aantonen dat u deze toestemming heeft gekregen.

Let op: indien u via een andere weg dan het TIS sollicitatieformulier of de toestemmingsmail wil vastleggen in het kader van de verwerking, dient u er zelf voor te zorgen dat u de toestemming ook kunt overhandigen. Achteraf toestemming vragen via de toestemmingmail is natuurlijk altijd mogelijk.

### Organisatorische en technische veiligheidsmaatregelen

Om de privacy van betrokkenen te waarborgen dient u inzichtelijk te maken welke organisatorische en technische maatregelen u heeft genomen. Dit houdt in dat u een procesbeschrijving dient te maken van de manier waarop u gegevens verwerkt. Afhankelijk van uw specifieke klantsituatie, zou dat als volgt kunnen zijn:

Processchema Tangram



## Werken volgens de GDPR (AVG) richtlijnen

---

Met de 2017.2 update heeft u in de Tangram software functionaliteit tot uw beschikking gekregen waarmee u meer controle heeft op het gebruikersmanagement. Hiermee heeft u de keuze gebruik te maken van de authenticatiemethode Active Directory. Indien u gebruik maakt van het interne authenticatiemechanisme, kunt u bijvoorbeeld minimale eisen stellen aan de kwaliteit van wachtwoorden van gebruikers. Het is sowieso verplicht met een wachtwoord te werken en wachtwoorden verlopen automatisch na de ingestelde periode. Tevens is via het data-log inzichtelijk welke personen bepaalde informatie hebben ingezien en/of bewerkt.

Tangram is verwerker van gegevens die u ten aanzien van de GDPR (AVG) wetgeving als verantwoordelijke verwerkt. Tangram maakt gebruik van een extern datacenter dat gevestigd is in Nederland. Het betreffende datacenter is ISO 27001 gecertificeerd, zodat geborgd is dat alle passende technische- en organisatorische maatregelen genomen zijn om de gegevens te beschermen.

Tot slot is aan te raden dat u een informatiebeveiligingsbeleid opstelt. In dit beleid kunt u alle maatregelen en middelen beschrijven op welke wijze u als organisatie omgaat met informatiebeveiliging breder dan alleen de beveiliging van persoonsgegevens.

### Data Protection Impact Assessment (DPIA)

Zodra uw beoogde gegevensverwerking waarschijnlijk een hoog privacy risico met zich meebrengt dient u een Data Protection Impact Assessment (DPIA) uit te voeren. In de DPIA wordt vastgelegd waarom, op welke manier en hoe lang er persoonsgegevens verwerkt worden. De DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te nemen om de risico's te verkleinen.

**TIP:** Een handreiking voor de [uitvoering van een PIA](#), de voorloper van de DPIA op de website van de beroepsorganisatie van IT-auditors (NOREA) treft u op de [website](#) van de Autoriteit Persoonsgegevens.

### Privacy by design & privacy by default

Belangrijke uitgangspunten in de AVG zijn 'privacy by design' en 'privacy by default'. Tangram neemt als leverancier van uw systemen hierin het voortouw. Maar ook voor uw eigen organisatie met bijvoorbeeld een website, medewerker-portaal of andere applicatie is dit van toepassing. **Privacy by design** houdt in dat u er al bij het ontwerpen van informatiesystemen en diensten voor zorgt dat persoonsgegevens goed worden beschermd. **Privacy by default** houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.

## Bewaartermijn

Een belangrijke uitgangspunt van de GDPR (AVG) is dat u persoonsgegevens dient te verwijderen of anonimiseren als identificatie niet meer noodzakelijk is voor het doel waarvoor deze gegevens zijn verstrekt. In de GDPR (AVG) wordt niet specifiek aangegeven hoelang u gegevens mag bewaren, tenzij daar een specifieke wettelijke grondslag voor is. Voor gegevens uit de salarisadministratie die fiscaal van belang zijn, geldt bijvoorbeeld een wettelijke bewaartermijn van zeven jaar. Voor loonbelastingverklaringen en kopie identiteitsbewijzen geldt een termijn van vijf jaar. Voor een personeelsdossier geldt: twee jaar na uitdiensttreding.

Op basis van de huidige richtlijnen van de Autoriteit Persoonsgegevens geldt voor sollicitatiegegevens (brief, formulier, CV, referenties, getuigschrift) een termijn van vier weken na de sluitingsdatum van de vacature. Indien de kandidaat toestemming geeft voor een mogelijke match met een passende vacature in de toekomst, dan geldt voor sollicitatiegegevens en gegevens uit psychologisch onderzoek een maximale bewaartermijn van één jaar. Deze bewaartermijnen zijn beschikbaar gekomen in de 2017.2 update (standaard in Compact, optioneel/afwijkend voor klanten met een Power applicatie).

Met de 2017.2 update (standaard in Compact, optioneel voor klanten met een Power applicatie) heeft u ook functionaliteit tot uw beschikking gekregen om via workflow kandidaten te anonimiseren. Belangrijk te weten is dat kandidaten niet automatisch in deze workflow worden aangeboden. Alleen kandidaten die toestemming hebben verleend, maar waarvoor de periode is verlopen, of de toestemming hebben ingetrokken, komen hier naar voren. Ook wordt er gekeken of de kandidaat voldoet aan een aantal voorwaarden:

- a. De kandidaat mag niet ook contactpersoon zijn.
- b. De kandidaat mag niet in een lopende procedure zitten.
- c. De kandidaat mag niet gekoppeld zijn aan een traject (indien van toepassing).

In de 2018.1 update (i.c.m. "GDPR Extra") gaan we nog een stap verder. De voorwaarden om te anonimiseren zijn gelijk gebleven, maar u krijgt daarbij ook de mogelijkheid kandidaten inclusief alle gegevens te verwijderen (N.B. deze functionaliteit was al beschikbaar in Roos Compact 2017.2).

Naast het anonimiseren kunt u ook specifiek sollicitatiegegevens verwijderen, voor die situaties waarbij de bewaartermijn van de betreffende gegevens is verlopen. Denkt u daarbij aan het verwijderen van oudere sollicitaties (motivatiebrieven en/of toelichting)



van kandidaten die nu in een lopende procedure zitten, of kandidaten die u heeft aangenomen of ook als contactpersoon werkzaam zijn bij een organisatie.

Ook nieuw in de 2018.1 update (i.c.m. "GDPR Extra") is de mogelijkheid om op een selectie van kandidaten via menu-opties de velden "Toestemming vragen" of "Toestemming ingetrokken - datum" te vullen. Met deze acties kunt u kandidaten handmatig opnemen in de workflow om kandidaten om toestemming te vragen of te anonimiseren / verwijderen.

## Rechten van betrokkenen

In de AVG krijgen betrokkenen meer rechten.

1. Het recht op data-portabiliteit. Het recht om persoonsgegevens over te dragen is nieuw ten opzichte van de Wbp.
2. Het recht op vergetelheid. Ook het recht om 'vergeten' te worden is nieuw.
3. Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien.
4. Recht op rectificatie en aanvulling: het recht om de persoonsgegevens die u verwerkt te wijzigen.
5. Het recht op beperking van de verwerking: het recht om minder gegevens te laten verwerken.
6. Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten.
7. Het recht om bezwaar te maken tegen de gegevensverwerking.

Daarnaast krijgen organisaties meer verantwoordelijkheden. Bijvoorbeeld om binnen één maand te reageren op verzoeken van mensen die hun rechten willen uitoefenen.

Tangram zal u met de 2018.1 update ondersteunen bij het voldoen aan het recht om gegevens in te willen zien en recht op data-portabiliteit. Daarbij krijgt u de mogelijkheid om met één druk op de knop alle relevante gegevens te exporteren, waarna u deze gegevens (na eventuele screening) kunt overhandigen aan de betrokkene.

## Meldplicht datalekken

De meldplicht voor datalekken was al van toepassing in de Wpb en deze is ook in de GDPR (AVG) opgenomen. Er is sprake van een datalek als per ongeluk of opzettelijk data verloren gaat, of in handen komt van derden die daartoe niet bevoegd zijn. Een datalek dient binnen 72 uur aan de Autoriteit Persoonsgegevens gemeld worden. Houdt het lek waarschijnlijk een hoog risico in voor de personen waar de gegevens betrekking op hebben? Dan moeten zij ook van het lek op de hoogte worden gesteld.

Belangrijke toevoeging in de GDPR (AVG) is dat datalekken moeten worden gedocumenteerd. De AVG stelt verplicht om alle datalekken intern te documenteren, óók datalekken die niet gemeld worden aan de toezichthouder. De persoon die privacygevoelige data voor opdrachtgevers verwerkt, is wettelijk verplicht alle datalekken aan hen te melden, zodat zij dit weer aan de toezichthouder kunnen melden. Met deze documentatie dient de Autoriteit Persoonsgegevens te controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Indien u zich niet houdt aan de eisen die de AVG stelt, kan er door de toezichthouder boetes en sancties worden opgelegd. De maximale boete is 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet, afhankelijk van welk bedrag hoger is.

### Tangram stappenplan

Tangram heeft ook nog een stappenplan beschikbaar, waarin wordt uitgelegd hoe de functionaliteit in het kader van de AVG werkt. U kunt deze raadplegen op de website van Tangram.

De Autoriteit Persoonsgegevens biedt instrumenten die u kunnen helpen met de naleving van de AVG, zoals richtlijnen die zijn opgesteld in samenwerking met de andere privacy toezichthouders in Europa.

Voor meer informatie:

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving>

Dit is een uitgave van:

# Tangram'

Disclaimer:

Tangram streeft er naar de informatie zo volledig en accuraat mogelijk weer te geven, maar is niet aansprakelijk voor de gevolgen voor een onjuiste interpretatie of weergave van deze informatie. De informatie kan gewijzigd worden zonder voorafgaande berichtgeving.

Tangram | Dr. s'Jacoblaan 26 | 3707 VK Zeist | 030 – 691 9171 | [www.tangram.nl](http://www.tangram.nl)