Yellow Yard
Recruitment software

Recruitment volgens de nieuwe regels

HANDOUT GDPR

Inhoudsopgave

	Pagina
General Data Protection Regulation	3
Definities	3
Privacy by Design	4
Actieve houding t.a.v. beveiliging	5
Voorbeeld: Cookies	5
GDPR voor Recruiters	6
Sourcing	6
Toestemming	6
Toegang	7
Termijnen	7
GDPR & Yellow Yard	8
Privacy-tab	8
Procedures & instellingen	8
Prullenbak	8
Toestemming	9
Batchmailing	9
Sollicitatieformulier	9
Privacy Statement	10
Template	12
GDPR & Jouw organisatie	13
Toestemming voor alle activiteiten	13
Beleid opstellen en collega's trainen	13
Register van Verwerking	13
Afsluitend	14

General Data Protection Regulation

De GDPR komt eraan! Maar wat betekent het nu eigenlijk? Er staat vanaf 25 mei 2018 veel te veranderen op het gebied van privacy. Met de inwerkingtreding van de General Data Protection Regulation zal ook het nodige in jouw dagelijkse bedrijfsprocessen moeten veranderen. In deze handout behandelen we de veranderende regelgeving en de invloed die dit heeft op jouw dagelijkse praktijk.

Definitie van partijen

We beginnen met de verschillende partijen. De **Betrokkene** is de natuurlijke persoon wiens privacy beschermd wordt. Dit wordt vooral bewerkstelligd door een aantal rechten die iedere Europese burger vanaf 25 mei 2018 krijgt. De Betrokkene mag vanaf dat moment gebruikmaken van 4 rechten:

- Recht op inzage
- Recht op rectificatie
- Recht op data-portabiliteit
- Recht op vergetelheid

Recht op inzage: wanneer jij gegevens bewaart van een kandidaat, is de kandidaat de Betrokkene. De Betrokkene mag op ieder moment vragen om een uitdraai van alle gegevens die jij in de loop der tijd hebt bewaard. Dus ook de beoordeling van het kennismakingsgesprek of je persoonlijke opmerking bij de ziekmelding.

Recht op rectificatie: wanneer blijkt na inzage van de gegevens dat er verkeerde gegevens vermeld staan, heeft de Betrokkene het recht deze aan te passen.
Recht op data-portabiliteit: wanneer de Betrokkene besluit de diensten van een andere partij te gaan gebruiken, mag de Betrokkene de gegevens kosteloos opvragen in een bruikbaar digitaal format (zoals XML of CSV). Deze gegevens mogen dan aangeboden worden aan de andere partij. Wanneer Betrokkene aanvullende eisen stelt aan het format, mag je daar administratieve kosten voor in rekening brengen.

Recht op vergetelheid: wanneer een Betrokkene niet langer van jouw diensten gebruik wil maken, heeft de Betrokkene het recht om ‘vergeten’ te worden. Dat betekent dat de Betrokkene in geen van je systemen teruggevonden mag worden. Alle gegevens die betrekking hebben op de Betrokkene moeten in beginsel vernietigd worden.

Dit laatste recht heeft echter wel een aantal uitzonderingen. Overheidsinstanties zijn bijvoorbeeld gevrijwaard om aan dit verzoek gehoor te geven. Daarnaast mag je gegevens bewaren voor statistisch onderzoek. Verder mag je, als er een gegronde reden bestaat, dit verzoek naast je neerleggen. De fiscale bewaarplicht is zo’n gegronde reden: voor de fiscus ben je verplicht een adequate (loon-)administratie te voeren. Dat betekent dat bewaartermijnen die hiervoor gelden boven de GDPR gaan.

Jij bent als belanghebbende organisatie de **Verwerkingsverantwoordelijke**. De partij die primair baat heeft bij het verzamelen van de gegevens. De Verwerkingsverantwoordelijke heeft voornamelijk plichten ten aanzien van de gegevensbescherming en -administratie. Dit betekent dat de Verwerkingsverantwoordelijke een Register van Verwerking opbouwt. In dit register staan alle onderliggende relaties met Verwerkers en de gegevens die zij voor Verwerkingsverantwoordelijke verwerken. Daarnaast voert de Verwerkingsverantwoordelijke actief beleid op beveiliging van gegevens en is de procedure voor het melden van datalekken helder omschreven. Van iedere Betrokkene heeft Verwerkingsverantwoordelijke schriftelijke toestemming beschikbaar voor het verwerken en inzetten van de gedeelde gegevens.

Verwerkers zijn partijen die de gegevens verwerken zonder daar zelf baat bij te hebben. Denk hierbij aan partijen als Mailchimp of je ATS-leverancier. Dit zijn partijen waarmee jij data deelt ten behoeve van het beter uitvoeren van jouw dienstverlening. Deze partijen hebben zelf geen recht om met de gegevens te werken, maar voeren op basis van de gegevens specifieke taken uit. Verwerkers mogen hiervoor ook **subverwerkers** aanstellen. Deze subverwerkers ondersteunen de Verwerker in het mogelijk maken van hun dienstverlening.

Privacy by Design

De wetgeving voorziet in een verandering van zienswijze. Met de komst van Big Data worden allerlei gegevens lukraak opgeslagen: je weet tenslotte nooit of je er nog iets aan hebt! En dat mag dus niet meer. Het is prima om na het verkrijgen van toestemming via het Privacy Statement de verkregen data volgens de afspraak voor jouw organisatie in te zetten. Mits deze data van belang is voor het kunnen uitvoeren van de dienstverlening. De beste vraag die je jezelf hierbij kunt stellen: heeft het nut om dit te weten van de Betrokkene en wordt het verlenen van mijn diensten hierdoor beter?

> Stel: jij schrijft een kandidaat in en vraagt naar de gezinssamenstelling. Met welk doel doe je dit? Kan jij de kandidaat beter van dienst zijn, omdat je nu weet dat zij een partner en kind heeft? Dit is niet per se nuttige informatie voor een klant en kan wellicht beter achterwege gelaten worden. Tegelijkertijd kan je daar een grondige reden voor hebben: je klant is specifiek op zoek naar jonge moeders om een betere binding met de doelgroep te hebben. Dan is het nuttig en mag je dit best opslaan in je systeem.

Privacy wordt door de invoering van de GDPR dus meer een samenwerking met de Betrokkene en de gegevens die je tijdens die samenwerking opslaat, sla je op met een specifiek doel en zijn daardoor in beginsel nuttig. In het kader van Privacy by Design weeg je dat voor elk gegeven af.

Actieve houding t.a.v. beveiliging

Onder de Wet Bescherming Persoonsgegevens had jouw organisatie een passieve plicht zorg te dragen voor een redelijke beveiliging van de opgeslagen gegevens. Dit verandert met de invoering van de GDPR aanzienlijk. Van jou wordt als belanghebbende partij verwacht dat jij de gegevens, die jij in feite in bruikleen hebt, actief verdedigt tegen bedreigingen van buitenaf.
Om dit goed te organiseren, maak je inzichtelijk welke gegevens je verwerkt en welke partijen hierbij een rol vervullen. Met deze partijen sluit je een verwerkersovereenkomst, waarin onder meer de beveiliging wordt besproken en het beleid ten aanzien van datalekken wordt neergelegd. Dit alles houd je bij in een Register van Verwerking.

Voorbeeld: Cookies

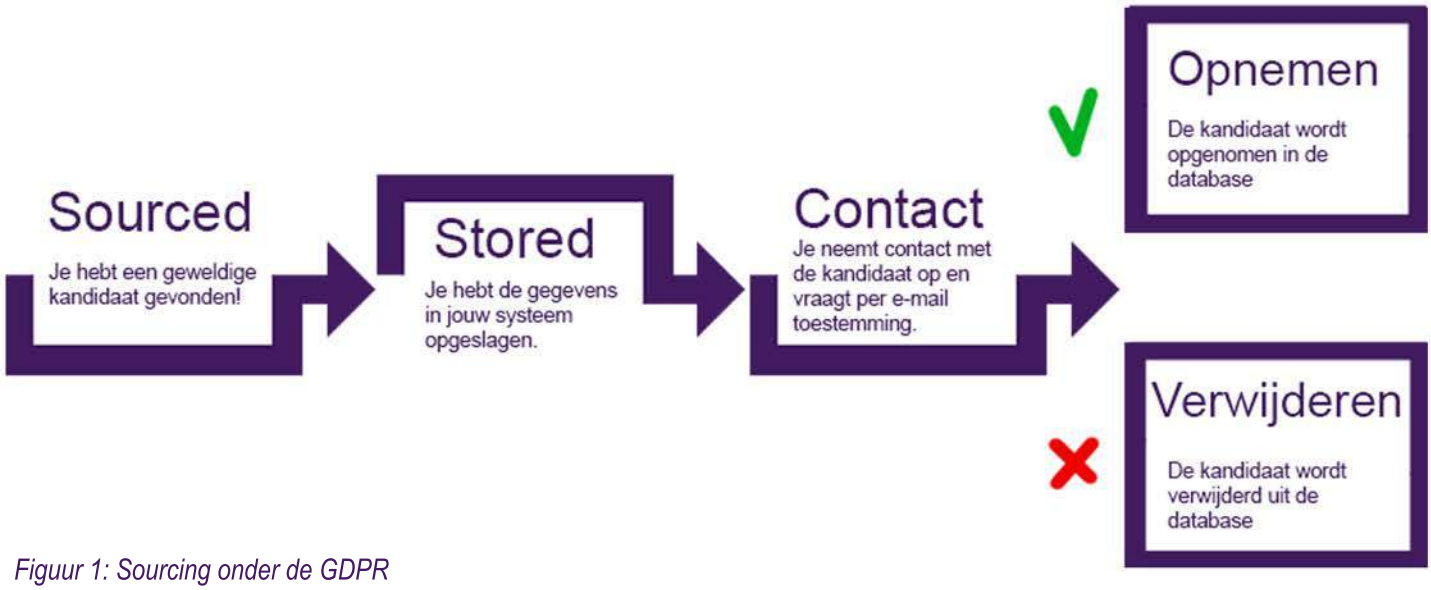
Een hands-on voorbeeld: tegenwoordig kom je op vrijwel elke website een cookie-wall tegen. Zonder acht te slaan op de inhoud klik je door en ga je akkoord. Want een keuze geeft de wall je toch niet. Dit mag vanaf 25 mei 2018 dus ook niet meer. Een klant of bezoeker moet actief toestemming geven om gevolgd te kunnen worden, de zogenaamde **opt-in**. In beginsel geeft iemand dus geen toestemming, de **opt-out**.
Je mag wel aangeven dat de kwaliteit van de beleving slechter is, wanneer er geen cookies ingeschakeld zijn. Kiezen voor een opt-out mag niet leiden tot een totale blokkade: de website blijft functioneren en bezoekers kunnen van alle functionaliteiten gebruik blijven maken.

GDPR voor Recruiters

De GDPR is natuurlijk niet alleen in het leven geroepen voor recruiters. Dat betekent dat veel van de wetgeving aan interpretatie onderhevig is. Hieronder zetten wij uiteen wat jij sowieso moet gaan doen als jij wilt voldoen aan de GDPR.

Sourcing

Het werven van kandidaten is de basis van jouw business. Maar hoe ga je om met de gegevens? Je vindt potentiële kandidaten via Linkedin, jobboards of andere kanalen en wilt hen benaderen. Maar hoe gaat het met de gegevens die je van hen opslaat? Je mag niet zomaar de gegevens opslaan voor onbepaalde termijn, ook niet als deze openbaar door de beoogde kandidaat worden gedeeld.
De huidige consensus stelt dat je voor een bepaalde termijn de gegevens mag verwerken, waarna je contact moet zoeken met de potentiële kandidaat en om toestemming moet vragen. In fig. 1 hebben we een schematische weergave voor je gemaakt.



Figuur 1: Sourcing onder de GDPR

Toestemming

Na het sourcen van je kandidaat moet je dus toestemming vragen. Deze toestemming moet schriftelijk gegeven worden, omdat je te allen tijde moet kunnen aantonen dat de kandidaat akkoord is gegaan. Deze toestemming verwerk je met de datum van toekenning in jouw systeem bij de specifieke kandidaat. De toestemming heeft een van tevoren vastgestelde termijn, waarna opnieuw om toestemming gevraagd moet worden of de gegevens uit het systeem verwijderd worden.

Toegang

Belangrijk: de kandidaat krijgt toegang tot zijn of haar gegevens. De kandidaat kan te allen tijde een verzoek indienen om zijn of haar gegevens te controleren. Dat betekent dat je jouw systemen hierop moet inrichten. Een kandidaat heeft toegang tot alle gegevens die jij bij hem of haar opslaat, dus ook gespreksverslagen en beoordelingen.

Termijnen

De GDPR voorziet niet in termijnen. Dat is op zichzelf ook verklaarbaar; geen enkele branche is hetzelfde en doorlooptijden van processen zijn sterk wisselend. Je mag dit dus zelf instellen. Dit betekent niet je simpelweg jaren achtereen prospects in je database mag laten staan zonder toestemming te vragen. De termijnen die jij wilt gebruiken, moeten verdedigbaar zijn. Zo is het prima verdedigbaar dat je een termijn aanhoudt van twee weken waarin een kandidaat benaderd moet worden om toestemming te geven. Het kost enige tijd om diegene te bereiken en terugkoppeling te krijgen. Drie maanden is daarentegen erg lang om contact met iemand te krijgen en een terugkoppeling van diegene te ontvangen.

De looptijd van de toestemming is een ander vraagstuk: wat is in jouw organisatie een normale doorlooptijd? Hoe ga je om met detachering? Wat als je een ZZP-er bemiddelt voor een opdracht van een jaar? Niet elke kandidaat zal binnen drie maanden aan het werk zijn, maar het is niet nodig dat de gegevens vijf jaar op de plank blijven liggen. Een termijn voor de toestemming van 1 of 2 jaar is, afhankelijk van jouw dagelijkse praktijk, verdedigbaar. Langer mag, mits je daar een gegronde reden voor hebt. In het geval van detachering mag je uitgaan van een voortdurende toestemming. **In je Privacy Statement zou je op kunnen nemen dat de toestemming voor de duur van de detachering wordt gegeven, met een minimale looptijd van 2 jaar bijvoorbeeld.**

GDPR & Yellow Yard

Binnen jouw Yellow Yard-omgeving verandert uiteraard ook het nodige om jou te faciliteren. In dit hoofdstuk gaan we dieper op de veranderingen in en bereiden we je voor op wat je van onze zijde mag verwachten.

Privacy-tab

Aan Yellow Yard wordt onder de kandidaat een nieuw tabblad toegevoegd. Dit tabblad is speciaal voor alle GDPR-gerelateerde zaken ingericht. Hierin kun je zien of een kandidaat toestemming heeft gegeven, wanneer dit is geweest, met welke versie van het Privacy Statement akkoord is gegaan en wanneer de toestemming afloopt. Verder kan in het tabblad bijgehouden worden welke verzoeken een kandidaat heeft ingediend.

Procedures & instellingen

Omdat elke organisatie zijn eigen procedures hanteert en eigen termijnen mag bepalen, krijgt de administrator toegang tot de instellingen van de Privacy-tab. Onder ‘Instellingen’ krijgt de administrator de mogelijkheid om de termijnen in te stellen voor sourcing en verwijdering uit de prullenbak. In jouw Yellow Yard-omgeving vind je aan de linkerkant van je scherm het tabblad “Blog”; waarin we je informeren over de nieuwste ontwikkelingen binnen dit thema.

Prullenbak

De GDPR draait op het versterken van de Betrokkene: als deze niet langer bemiddeld wil worden door jouw organisatie, moet je hem of haar kunnen verwijderen. Daarom krijg jij binnen Yellow Yard de mogelijkheid om kandidaten te verplaatsen naar de ‘prullenbak’. In de prullenbak worden de gegevens deels geanonimiseerd. De kandidaat blijft herkenbaar bij naam, maar de overige (CV-)gegevens zijn niet langer beschikbaar. Indien een kandidaat in de prullenbak staat, is het dus nog steeds mogelijk om rapportages uit te draaien, gebaseerd op zijn of haar data (denk hierbij aan aantallen sollicitaties op een vacature).

De kandidaat op een vacature voorstellen is op dat moment ook niet langer mogelijk. Wanneer je zeker bent van je selectie, kan je de prullenbak legen en worden de geselecteerde kandidaten definitief verwijderd. Wanneer de kandidaat per direct uit het systeem verwijderd moet worden, kan dit ook via de prullenbak. Na de selectie kan in de prullenbak iedere individuele kandidaat apart verwijderd worden. Het is ook mogelijk meerdere kandidaten in één keer te verwijderen.

Toestemming

Jij hebt natuurlijk een uitgebreide database opgebouwd met kandidaten en krijgt regelmatig nieuwe kandidaten binnen via je sollicitatieformulier. Gezien de GDPR moet je wel toestemming krijgen van zowel bestaande als nieuwe kandidaten voor het verwerken en opslaan van hun gegevens. Om dit te bewerkstelligen kun je gebruik maken van onderstaande mogelijkheden.

Batch-mail

Al je kandidaten om toestemming vragen kan een behoorlijke tijdrovende klus worden. Yellow Yard biedt je de mogelijkheid je bestaande kandidaten door ons te laten mailen. Op deze manier voorkom je dat je e-mailserver gerapporteerd wordt als spamserver.

Vraag hier een offerte aan

Voorbeeld van de batchmail

Sollicitatie formulier

Jouw sollicitatie formulier moet aangepast worden om te voldoen aan de nieuwe Privacy wetgeving. Behalve het opnieuw beoordelen van de gegevens die je de sollicitant vraagt te delen; moet je, je Privacy Statement aanpassen aan de nieuwe eisen van de GDPR. Het toevoegen van het nieuwe Privacy Statement aan het sollicitatie formulier kan Yellow Yard voor jou verzorgen.

Wanneer een nieuwe sollicitant zich meldt via het formulier, wordt onder de kandidaat in Yellow Yard bijgehouden of en wanneer de kandidaat toestemming gegeven heeft. De administratie voor de gegeven toestemming is daarmee direct verzorgd.

Vraag hier een offerte aan

Privacy Statement

Het Privacy Statement wordt een stuk complexer. Maar waar moet het allemaal precies aan voldoen? Hieronder hebben we voor jou de regels op een rijtje gezet:

Duidelijke taal
Beknopt, begrijpelijk en toegankelijk. Iedereen die toestemming moet geven, moet het kunnen begrijpen.

Tenaamstelling
Je maakt jezelf bekend als degene die vraagt om de toestemming. Je bent de belanghebbende en je stelt jezelf dus even netjes voor.

Doel van de te verzamelen gegevens
Waarom wil jij gegevens verzamelen? Wat wil je ermee gaan doen? Je beschrijft kort, bondig en volledig met welk doel je de gegevens verwerkt. Je mag dit nog wel ruim beschrijven: ‘alle activiteiten rondom arbeidsbemiddeling’ of ‘communicatie tussen verschillende partijen ten behoeve van de arbeidsbemiddeling’.

Beschrijving van de gegevens
Onder de GDPR moet jij een duidelijk beeld hebben van de gegevens die jij verwerkt. In het kader van transparantie heb je voor de Betrokkene een overzicht beschikbaar van de gegevens die je verwerkt.

Wie gaat er mee werken?
Elke partij waar jij mee samenwerkt voor het verwerken van de gegevens van Betrokkene moet inzichtelijk zijn voor de Betrokkene. Dit mag ook een overzicht zijn op bijvoorbeeld je website waarnaar verwezen wordt.

Termijnen
Je geeft in het Privacy Statement aan hoe lang de toestemming geldt. In bepaalde gevallen weet je niet hoe lang het zal zijn. Een kandidaat kan bijvoorbeeld opgenomen willen worden in een mailinglijst met de laatste vacatures. Op dat moment is het voor jouw bedrijfsproces van belang dat je de gegevens van de kandidaat gebruikt .

Aangeven dat de Betrokkene mag wijzigen, inzien en verwijderen
De Betrokkene krijgt in de GDPR meer rechten. Daar dien je hem of haar aan te herinneren in het Privacy Statement. De Betrokkene mag de gegevens inzien, rectificeren, verwijderen of overdragen aan een andere partij op ieder moment dat de Betrokkene dit wil. Jij bent verplicht de gevraagde gegevens op dat moment aan de Betrokkene te overhandigen.

Gerechtvaardigd doel vs. bezwaar bij verwijdering
Zoals gezegd heeft de Betrokkene het recht zijn of haar gegevens te laten verwijderen. Wanneer jij een gerechtvaardigd doel hebt de gegevens wel te bewaren (door een fiscaal-administratieve plicht, bijvoorbeeld), hoef jij aan dit verzoek geen gehoor te geven. Dit benoem je ook in je Privacy Statement.

Klagen bij Autoriteit Persoonsgegevens
In je Statement geef je aan bij wie de Betrokkene terecht kan met klachten. Dit is uiteraard de Autoriteit Persoonsgegevens.

Geen contract
Je geeft duidelijk aan of er sprake is van een contract. In het geval van kandidaten zal hiervan geen sprake zijn. Toch moet je dit specifiek benoemen. Het verlenen van toestemming kan een voorwaarde zijn voor het gebruik maken van de dienstverlening.

Geautomatiseerde besluitvorming
Wanneer je gebruik maakt van geautomatiseerde besluitvorming moet je dit vermelden en aangeven hoe dit van invloed is.

Template
Om je een idee te geven van een Privacy Statement dat in beginsel voldoet aan de eisen, hebben wij hieronder een voorbeeld opgesteld. Dit voorbeeld is bewust beknopt en begrijpelijk geschreven. Wij hebben ervoor gekozen een termijn van 24 maanden aan te houden voor dit voorbeeld.

NB: Dit voorbeeld is bedoeld als inspiratie, een manier om met de nieuwe regels om te gaan. *Yellow Yard Recruitment Software B.V. staat niet in voor de volledigheid van dit voorbeeld.*

Privacy Statement

[[Jouw bedrijfsnaam] mag mijn gegevens gebruiken voor de duur van 24 maanden. Met deze gegevens staat het [jouw bedrijfsnaam] vrij te werken.
Ik mag mijn gegevens altijd:

- Inzien
- Aanpassen
- Overdragen aan een andere partij
- Laten verwijderen

Ik begrijp dat [Jouw bedrijfsnaam] kan besluiten mijn gegevens niet te verwijderen als er sprake is van administratieve plichten.
[Jouw bedrijfsnaam] slaat mijn persoonsgegevens, arbeids- en opleidingsgeschiedenis en andere bij de dienstverlening passende gegevens op. Hier bevindt zich het overzicht met alle gegevens.
[Jouw bedrijfsnaam] mag mijn gegevens delen met andere bedrijven in de uitvoering van hun taken. Ik begrijp dat ik op deze pagina kan zien met welke partijen zij samenwerken. Mijn toestemming is geen onderdeel van een contract, maar wel nodig voor de uitvoering van de dienstverlening van [jouw bedrijfsnaam]. Als er in de toekomst iets niet gaat zoals afgesproken met mijn gegevens weet ik dat ik naar de Autoriteit Persoonsgegevens kan gaan om mijn zaak aan te dragen.

Register van Verwerking

Jij bent verantwoordelijk voor het goed beveiligen van de gegevens van jouw kandidaten. Daarom houd jij in een Register van Verwerking bij. Dit Register moet wel voldoen aan bepaalde kenmerken en voorwaarden. Op **ICTrecht.nl** vind je een goed overzicht van de specifieke onderdelen.

GDPR & Jouw organisatie

Wat moet er nu gebeuren:
• Je moet je Privacy Statement aanpassen
• Je moet bestaande kandidaten vragen of zij **actief akkoord** willen gaan met de verwerking van hun gegevens
• Kandidaten die geen akkoord geven, dien je te anonimiseren en/of verwijderen
• Je moet transparant zijn over het gebruik van de gegevens en de onderlinge verbanden die op de achtergrond spelen
• Nieuwe sollicitanten moeten toestemming hebben gegeven voor het opslaan en verwerken van hun gegevens

Toestemming voor alle activiteiten

Onder de GDPR ben jij verantwoordelijk voor de beveiliging van alle persoonsgegevens voor elke activiteit. Dit betekent dat het niet alleen gaat over je primaire activiteiten, maar ook over secundaire activiteiten waarbij je gebruik maakt van andermans gegevens. Denk hierbij bijvoorbeeld aan de nieuwsbrief. Welke partijen krijgen die gegevens in handen? Ga daarom na bij welke activiteiten in jouw organisatie gebruik gemaakt wordt van gegevens van de Betrokkene. Als bij deze activiteit gebruik gemaakt wordt van een verwerker dien je met deze partij een **verwerkersovereenkomst** af te sluiten.

Beleid opstellen en collega's trainen

Je zou het bijna vergeten, maar de GDPR is vooral bedoeld om organisaties een actieve rol te geven in de bescherming van persoonsgegevens. Dat is dan ook de taak die je nu ten deel valt. Er wordt van jou als organisatie verwacht dat beleid wordt opgesteld om persoonsgegevens van Betrokkenen zo goed mogelijk te beschermen. Denk hierbij aan interne regels over hoe jullie omgaan met een datalek of een verzoek tot data-portabiliteit. Dat betekent ook dat elke medewerker hiervan op de hoogte moet zijn: hoe werk je veilig met andermans gegevens, wat te doen bij verzoeken in het kader van de GDPR en wat gebeurt er als je het vermoeden hebt van een datalek? Zorg daarom voor een goede interne training, waarbij iedere collega scherp in de gaten heeft wat de risico's zijn.

Register van Verwerking

Het opgestelde beleid is onderdeel van het Register van Verwerking. Dit Register is onder meer een verzameling van alle Verwerkersovereenkomsten die jij hebt afgesloten met jouw software leveranciers. In dit register houd je overzichtelijk bij welke gegevens je verwerkt in samenwerking met welke leverancier. De reden om dit register op te bouwen is het minimaliseren van de aansprakelijkheid. Als Verwerkingsverantwoordelijke heb je hiermee de juiste voorbereiding getroffen. In geval van een incident zal de Autoriteit Persoonsgegevens hier rekening mee houden bij het opleggen van sancties.
Yellow Yard heeft al haar klanten eind maart de Verwerkersovereenkomst toegezonden. Heb je deze niet ontvangen? Maak dan een ticket aan in jouw Yellow Yard omgeving.

Afsluitend

Met deze handout hopen wij jou meer inzicht te hebben gegeven in de veranderingen binnen jouw processen, Yellow Yard en de achterliggende gedachtes vanuit de nieuwe wetgeving.

De nieuwe wet vraagt veel voorbereiding van ons als jouw ATS-leverancier en van jou als professional in de arbeidsbemiddeling.

In de uitvoering van jouw werk zal je met regelmaat tegen vraagstukken aanlopen die verband houden met de nieuwe wetgeving. Vanuit Yellow Yard doen wij ons uiterste best om jou snel en doeltreffend op de hoogte te houden van nieuwe ontwikkelingen binnen dit thema.
Belangrijk is; dat hiermee jouw eigen verantwoordelijkheid om goed geïnformeerd te blijven uiteraard niet komt te vervallen.

Disclaimer: Deze handout is ontwikkeld als interpretatie op de wetgeving. Afwijkingen kunnen ontstaan voor, tijdens of na de invoering van de wetgeving. Yellow Yard heeft bij het ontwikkelen van dit product verschillende bronnen gebruikt en zorgvuldig advies opgesteld, maar kan niet garanderen dat dit in specifieke gevallen door uitvoerende instanties anders wordt geïnterpreteerd. Aan deze hand-out kunen derhalve geen rechten worden ontleend en wij adviseren bij bedrijfs-specifieke vraagstukken altijd een jurist in te schakelen.