Voorbereid op weg naar de AVG in 9 korte artikelen

Voorbereid op weg naar de AVG: Is de nieuwe privacywetgeving voor onze organisatie relevant? *Dit is de 1ste van 9 korte artikelen over de nieuwe privacywetgeving: de Algemene Verordening Gegevensbescherming (AVG). In de komende artikelen behandelen we de belangrijkste 8 thema's uit de AVG.*

Elk artikel gaat nader in op één van de thema's en geeft specifieke informatie over de verandering in de wet en de betekenis daarvan in de praktijk. Dit eerste artikel gaat nader in op de AVG zelf;

'Is de regelgeving wel zo nieuw als iedereen zegt?'
De AVG is op 24 mei 2016 in werking getreden. Om maar gelijk met de deur in huis te vallen: ja, de AVG is van toepassing op uw organisatie. De leden van Sociaal Werk Nederland zijn alle sociaalwerkorganisaties. Deze sector verwerkt gegevens van cliënten en in veel gevallen zelfs bijzondere gegevens, zoals medische gegevens en het burgerservicenummer (BSN). Dat is precies waar de AVG zich op richt. U krijgt tot 25 mei 2018 de tijd om te voldoen aan de nieuwe wet- en regelgeving en uw organisatie hieraan aan te passen. De AVG heeft als doel het reguleren van de omgang met persoonsgegevens, oftewel de verwerking van persoonsgegevens.

Voorheen waren de regels rond privacy in een Europese richtlijn uitgewerkt, waar de Wet bescherming persoonsgegevens (Wbp) op gebaseerd is. Veel van de basisprincipes en concepten uit de AVG zijn terug te vinden in de Wbp. Er is echter wel een aantal verbeteringen doorgevoerd waar u rekening mee moet houden.

Het is belangrijk om u nu alvast voor te bereiden om de overgang naar de nieuwe wet- en regelgeving vlot te laten verlopen. Zorg dat u de steun heeft van uw bestuur en uw management. Er moeten bijvoorbeeld nieuwe procedures worden ingericht om de rechten van betrokkenen te garanderen. U moet wellicht een Functionaris voor Gegevensbescherming aanstellen en een privacy-governance-structuur inrichten. Hoe dan ook: de AVG heeft impact op uw budget, IT-afdeling, medewerkers, beleid en communicatie.

U zult er rekening mee moeten houden dat sommige bepalingen uit de AVG meer impact hebben op uw organisatie dan andere. Het is geen 'one-size-fits-all'-wetgeving. Maatwerk is 'the key'!

Volgende week wordt ingegaan op de rol van de Functionaris voor Gegevensbescherming. Heeft u als organisatie een dergelijke functionaris écht nodig?

Artikel 2: Heeft mijn organisatie wel écht een Functionaris voor Gegegevensbescherming nodig?

1. Inrichting privacyorganisatie

Een belangrijke rol binnen de privacyorganisatie is weggelegd voor de privacy officer of 'Functionaris voor Gegevensbescherming' (FG). Maar wat moet deze eigenlijk doen en wanneer is deze verplicht? En met het aanstellen van een FG bent u er niet, want wie is er bestuurlijk eindverantwoordelijk voor privacy? En wat is de rol van stafmanagers (bijvoorbeeld op het gebied van HR, ICT en inkoop) en van de lijnmanagers? Het is belangrijk om vast te stellen welke plaats een FG inneemt binnen de structuur en het beleid van uw organisatie en wat de logische taken, rollen en verantwoordelijkheden zijn voor medewerkers en managers.

Verplicht?
In een aantal situaties verplicht de AVG dat u een FG aanstelt. Maar, ook als dit wettelijk niet verplicht is, kan het aan te bevelen zijn iemand aan te wijzen die verantwoordelijkheid draagt voor het naleven van de privacyregels. Het is ook mogelijk om een externe privacy officer of FG aan te wijzen. Kijk wat passend is voor uw organisatie.

Zelf afwegen
Het is belangrijk om te beoordelen of er binnen uw organisatie een dergelijke functionaris moet worden aangesteld. De leden van Sociaal Werk Nederland zijn allen sociaalwerkorganisaties. In veel gevallen zal in deze sector sprake zijn van verwerking van bijzondere persoonsgegevens op grote schaal. Wat precies wordt bedoeld met

‘grootschalig’ vertelt de AVG niet. Het is ook lastig om hier een getalscriterium aan te hangen. Er is dus een groot grijs gebied waarin u zelf moet bepalen of u een FG aanstelt. Meer over de afweging die u als organisatie moet maken, vindt u in de blog ‘Licht in de duisternis: wel of geen Functionaris voor Gegevensbescherming?’

Niet verplicht, maar toch verstandig?
Als u niet verplicht bent er een aan te stellen, kan het nog steeds verstandig zijn om een functionaris aan te wijzen. Dit zal dan vaak gepaard gaan met het vaststellen van de rollen en verantwoordelijkheden van de, bij privacy betrokken, functionarissen zoals de security officer, juridische zaken, ICT e.d.

Hiervoor kan gebruik gemaakt worden van het zogenaamde RACI-model. Dit is een matrix die gehanteerd wordt om de rollen en verantwoordelijkheden van de personen weer te geven. In de matrix staan dan op de horizontale as de namen van de personen of de functionele rollen, en op de verticale as de op te leveren resultaten, betrokken processen of activiteiten. Zo is voor iedereen duidelijk hoe de verantwoordelijkheden rondom privacy zijn belegd.

Artikel 3: Weet u welke gegevens u verwerkt en mag u die gegevens eigenlijk wel hebben?

2. Inzicht in verwerkingen & grondslagen

Uw organisatie voert verschillende types van gegevensverwerkingen uit. De leden van Sociaal Werk zijn allen sociaalwerkorganisaties. Grote kans dat uw dus gegevens over cliënten in een dossier bewaard, dat vrijwilligers gegevens van cliënten bewerken en dat u gegevens over uw eigen medewerkers deelt met een extern (loon)administratiekantoor. Het is belangrijk om inzicht te hebben in deze verschillende verwerkingen omdat u zeker moet weten dat u deze gegevens ook inderdaad mag gebruiken. Dit doet u in het zogenaamde ‘register van de verwerkingsactiviteiten’ (hierna: register).

U moet zorgvuldig in kaart brengen welke persoonsgegevens u bijhoudt, waar deze vandaan komen en met wie u deze hebt gedeeld. U moet dus verwerkingen in een actueel en volledig overzicht registreren en bijhouden. Per verzameling van persoonsgegevens moet de nodige informatie worden bijgehouden, zoals de grondslag, wie eventuele verwerkers zijn en hoe lang gegevens mogen worden bewaard. Hoe pakt u dit nu in de praktijk aan?

In de eerste plaats moet u een passende vorm voor het register kiezen. De meest praktische is een Wordbestand of Excelsheet. Voor de gemiddelde organisatie zal dit ook

voldoende zijn. Hoe groter de organisatie, of hoe meer verzamelingen bij diverse afdelingen liggen, hoe groter de behoefte aan gespecialiseerde tools.

In de tweede plaats moet u nagaan hoe u de volledigheid van het register kunt controleren. U kunt er niet van uitgaan dat iedereen uit zichzelf komt melden waar zich persoonsgegevens bevinden. Persoonsgegevens bevinden zich vaak bij bijvoorbeeld Personeelszaken (werving & selectie, arbeidsgerelateerde administraties), ICT (smoelenboek, active directory, ICT servicedesk) en Facilitair Management (camera's, klachtenafhandeling, bezoekersregistratie).

In de derde plaats zult u moeten aangeven wie verantwoordelijk is voor het vullen van het register. Het maakt de AVG niet uit wie intern het register vult. Het is logisch om, zeker bij grotere organisaties, het register decentraal te laten vullen (bijvoorbeeld één aanspreekpunt bij HR, één aanspreekpunt bij ICT, één aanspreekpunt binnen primair proces A, etcetera).

In de vierde en laatste plaats moet u nadenken over hoe u de actualiteit van het register kunt waarborgen. Uw organisatie staat niet stil. De dag nadat uw organisatie met veel pijn en moeite versie 1.0 van het register heeft afgerond, is het waarschijnlijk alweer achterhaald. Het hebben van een register is niet een 'projectje' dat je kunt afronden, het leidt echt tot een permanente beheertaak.

Naast een register van verwerkingsactiviteiten zult u, van de verschillende soorten gegevensverwerkingen die u daarin hebt vastgelegd, ook de wettelijke grondslag moeten identificeren. Ga hierover desnoods in overleg met een jurist, het is immers een zeer specialistische taak.

Artikel 4: Wisselt u gegevens over cliënten uit in een netwerk met anderen?

3. Verantwoordelijke & verwerker

Het is belangrijk om vast te stellen of andere organisaties persoonsgegevens voor u verwerken (de zogenaamde 'verwerker'). Als dit het geval is, bent u voor de privacywet de 'verwerkingsverantwoordelijke' en is het belangrijk dat u duidelijke afspraken maakt over de wijze waarop deze 'verwerker' omgaat met de persoonsgegevens die zij voor u verwerken. Deze afspraken kunnen vastgelegd worden in een verwerkersovereenkomst. U zult ook moeten voorzien in adequate procedures om datalekken op te sporen, te rapporteren en te onderzoeken. Hoe pakt u dit gestructureerd aan?

Eerst bepaalt u de 'verwerkingsverantwoordelijke'. Daarvoor moet u eerst weten welke (bijzondere) persoonsgegevens u verwerkt. In artikel 3 is hieraan aandacht besteed. U

heeft immers de verwerkingen vastgelegd in een register. Deze kan dus als basis dienen. De volgende vraag is wie de 'verwerkingsverantwoordelijke' is en wie de 'verwerker'. De privacywetgeving stelt dat degene die het doel en de middelen bepaalt in privacy termen 'de verwerkingsverantwoordelijke' is. Is dat het geval dan zult u het initiatief moeten nemen tot het sluiten van een verwerkersovereenkomst. Inventariseer dus per partij met wie u persoonsgegevens uitwisselt en wie het doel en de middelen bepaalt. Beide partijen hebben specifieke plichten om de beveiliging van persoonsgegevens goed te regelen. Privacy is immers teamwork.

Als u vastgesteld heeft in welke situaties u verantwoordelijke bent, is het van belang dat u met de verwerker een verwerkersovereenkomst gaat sluiten. In de AVG staan afspraken die u verplicht moet maken met uw verwerker. Ga in overleg met een jurist, dit is immers een specialistische taak.

Vervolgens is van belang om met de verwerker te kijken naar welke beveiligingsmaatregelen er door de verwerker getroffen moeten worden, passend bij het soort gegevensverwerking. U doet er verstandig aan ook deze contractueel vast te laten leggen en de ICT-afdeling, de systeembeheerder of de security officer met dit onderdeel mee te laten kijken.

Als laatste is het inrichten van een datalekprotocol belangrijk. Het belangrijkste daarbij is dat u de medewerkers informeert over wat een beveiligingsincident en een datalek is. Bijvoorbeeld via een interne nieuwsbrief, het intranet of een ander communicatiemiddel. Vervolgens is het belangrijk dat medewerkers een beveiligingsincident of datalek kunnen melden op eenvoudige en toegankelijke wijze. Dit kan bijvoorbeeld via een formulier op intranet. Ook zult u deze meldingen moeten registreren en daarom is het aan te bevelen een register aan te leggen waarin u de meldingen vastlegt.

Artikel 5: Moet ik eigenlijk wel steeds een Privacy Impact Assessment uitvoeren?

4. Privacy Impact Assessment

De zogenaamde 'gegevensbeschermingseffectbeoordeling', zoals de AVG de PIA noemt, zal binnen uw organisatie moeten worden uitgevoerd als sprake is van verwerkingen met een 'verhoogd risico'. De leden van Sociaal Werk zijn allen sociaalwerkorganisaties die veelal bijzondere persoonsgegevens verwerken. Grote kans dat er dus sprake is van een verhoogd risico op het schenden van de privacy en dat dús een PIA nodig is. Het is belangrijk om als organisatie privacyrisico's van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld te brengen. Het uitvoeren van een PIA is daarvoor het geëigende middel.

De zogenaamde ‘gegevensbeschermingseffectbeoordeling’, zoals de AVG de PIA noemt, zal binnen uw organisatie moeten worden uitgevoerd als sprake is van verwerkingen met een ‘verhoogd risico’. De leden van Sociaal Werk zijn allen sociaalwerkorganisaties die veelal bijzondere persoonsgegevens verwerken. Grote kans dat er dus sprake is van een verhoogd risico op het schenden van de privacy en dat dús een PIA nodig is. Het is belangrijk om als organisatie privacy-risico’s van een project in een vroeg stadium op een gestructureerde en heldere manier in beeld te brengen. Het uitvoeren van een PIA is daarvoor het geëigende middel.

Er is geen vaste manier om een PIA uit te voeren. De AVG stelt wel een aantal minimale eisen. Er bestaan ook verschillende methodes om een PIA uit te voeren. Kies zelf welke methode voor uw organisatie het meest geschikt is en voldoet aan de voorwaarden uit de AVG. Om te bepalen of er een PIA moet worden uitgevoerd is het goed om eerst de PIA ‘drietrapsraket’ door te nemen. Deze bestaat dus uit drie stappen om te bepalen of een PIA überhaupt noodzakelijk is.

Voer als eerste een globale beoordeling uit op de verwerkingen die u uitvoert. Beoordeel welke risico’s er kleven aan deze verwerkingen. Uit deze beoordeling kan naar voren komen dat er waarschijnlijk géén hoog risico kleeft aan een specifieke verwerking (bijvoorbeeld omdat geen persoonsgegevens worden verwerkt). Er kan ook naar voren komen dat er mogelijk wél een (hoog) risico kleeft aan de verwerking. In het eerste geval hoeft u niets te doen. In het tweede geval voert een uitgebreide PIA uit. Het resultaat van deze stap is een inzicht in de mogelijke risico’s ten aanzien van privacy. Het is logisch (maar op zich niet verplicht) om verbeterpunten te benoemen en zelfs concrete aanbevelingen te doen. Uit de PIA kan naar voren komen dat het hoge risico niet of juist wel kan worden beperkt met redelijke middelen. Als het risico kan worden beperkt, zorg dan dat u de passende maatregelen neemt. Kan het risico echter niet worden beperkt, raadpleeg dan de toezichthouder, de Autoriteit Persoonsgegevens.

Het uitvoeren van een PIA wordt vaak gezien als een verplicht ‘vinkje’ dat moet worden gehaald. Het gaat natuurlijk niet om het uitvoeren van de PIA, het gaat om wat u doet met de resultaten. Het is dan ook zaak om in uw methodiek te borgen wie verbeterpunten of aanbevelingen oppakt en monitort.

Bij voorkeur wordt de PIA uitgevoerd door iemand die begrijpt hoe de privacybegrippen passen op het bedrijfsproces. Formeel gezien is het niet de FG die een PIA zou moeten uitvoeren. De FG is wel degene die adviseert over de PIA en de prestatie ervan monitort.

Artikel 6: Wat zijn nu precies ‘passende en organisatorische maatregelen’ om persoonsgegevens zo goed mogelijk te beschermen?

5. Beveiliging

De AVG heeft het over zogenaamde ‘passende technische en organisatorische maatregelen’ ter beveiliging van persoonsgegevens. Uw cliënten én medewerkers moeten er immers op kunnen vertrouwen dat hun persoonsgegevens optimaal worden beveiligd. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van deze gegevens. U zult zelf maar slachtoffer zijn van identiteitsfraude… Organisaties die persoonsgegevens (gaan) verzamelen, moeten (vooraf) nadenken over de beveiliging hiervan. Dit is een continu proces: beveiliging van persoonsgegevens moet een blijvend punt van aandacht zijn.

Beveiliging wordt ook steeds belangrijker, zo bleek wel uit de vele datalekken bij ziekenhuizen, zorginstellingen, maar ook leasemaatschappijen. Ook de grote WannaCry-cyberaanval staat misschien nog wel vers in het geheugen. Uit deze aanval bleek dat het soms in kleine dingen zit, zoals het tijdig updaten van de systemen. Beveiliging blijft echter een specialisme op zich en het is dan ook belangrijk om tijdig de juiste expertise in huis te halen om uw organisatie te beschermen.

De verwerkingsverantwoordelijke zal moeten kunnen aantonen dat er passende technische en organisatorische maatregelen zijn genomen om de persoonsgegevens te beveiligen. Bij technische maatregelen kunt u denken aan het encrypten of pseudonimiseren van de gegevens. Bij organisatorische maatregelen kunt u denken aan beveiliging door toegangspasjes. Deze maatregelen moet u vastleggen in beleid en natuurlijk moet u dit beleid in de praktijk ook echt uitvoeren. Door beleid op te stellen en deze te implementeren kunt u aantonen dat u op dit punt aan de eisen uit de AVG voldoet. Onderwerpen in het beleid die voor vrijwel iedere situatie nodig zijn;

- logische toegangsbeveiliging, welke mensen mogen welke toegang hebben
- Versleuteling
- Fysieke beveiliging

- Continuïteit en beschikbaarheid
- Logging en monitoring

Documenteer dus, in samenwerking met andere disciplines (HRM, ICT, Juridische Zaken e.d.) hoe uw organisatie omgaat met de bescherming van persoonsgegevens. Dit beleid bevat gedetailleerde informatie en beschrijft interne processtappen. Betrek bij het opstellen en uitvoeren van het beleid de functionaris gegevensbescherming en zorg dat het beleid periodiek wordt geëvalueerd. Overigens is het maken van beleid alleen vereist als dat in verhouding staat tot de activiteiten. Bij eenvoudige verwerkingen is uitgebreide documentatie niet nodig en kan worden volstaan met eenvoudiger beleid dan bij meer complexe verwerkingen. Voor een blijvend passend beveiligingsniveau is inbedding van de zogeheten plan-do-check-act-cyclus voor beveiliging in de dagelijkse praktijk van de organisatie noodzakelijk.

Artikel 7: 'Privacy by Design' en 'Privacy by Default'; moet ik er echt wat mee?

6. Privacy by design/default

Gegevensbescherming door ontwerp, in het Engels 'privacy by design', houdt in dat de voor verwerking gebruikte mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van betrokkenen en de vereisten uit de AVG. 'Privacy by default' betekent dat de standaardinstellingen in uw systemen zo zijn gekozen dat de privacy maximaal wordt geborgd. Privacy by design is voor veel privacy officers een moeilijk onderwerp. Er zijn veel theoretische handvatten, maar het in de praktijk toepassen hiervan is vaak complex. Maak daarom uw organisatie vertrouwd met de uitgangspunten van privacy by design en privacy by default en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

De begrippen privacy by design en privacy by default worden vaak in één adem genoemd, maar hebben verschillende betekenissen.

Privacy by design houdt in dat u die technische en organisatorische maatregelen neemt om ervoor te zorgen dat u – als standaard – alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Het idee van privacy by design is om in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens te borgen. Bij de ontwikkeling van producten en/of diensten moet vooraf al aandacht zijn voor belangrijke privacy-beginselen als dataminimalisering en transparantie. Maak in het ontwikkelproces van ICT-producten

en -diensten al gebruik van privacy-verhogende maatregelen (ook wel privacy enhancing technologies of PET genoemd).

Privacy by default houdt in dat u die technische en organisatorische maatregelen neemt die ervoor zorgen dat de standaardinstelling de meest privacy-vriendelijke is. Denk daarbij aan instellingen op een social media profiel. Bij goed 'privacy by default' inrichten is het standaard zo dat u niks deelt, tenzij u het zelf aanpast. Dit principe van het afschermen van persoonsgegevens geldt voor alle ICT-toepassingen: van browser-instellingen tot een bedrijfs-app.

Maak uw organisatie nu al vertrouwd met de uitgangspunten van privacy by design en privacy by default. Ga na hoe u deze beginselen binnen uw organisatie kunt invoeren. Heeft uw organisatie bijvoorbeeld een app, zorg dan dat deze niet de locatie van gebruikers laat registeren als dat niet nodig is. Verzamelt u in uw organisatie leeftijdsdata? Ga dan eens na of u echt de leeftijd nodig hebt, of een bepaalde leeftijdsgrens (wel/niet ouder dan 18, wel/niet met pensioen).

Artikel 8: Welke rechten hebben cliënten eigenlijk als het gaat om hun privacy?

7. Rechten van betrokkenen

Onder de AVG krijgen betrokkenen meer en verbeterde privacy-rechten. U moet er dus voor zorgen dat zij hun privacy-rechten goed kunnen uitoefenen. Houd met name rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Betrokkenen moeten hun gegevens makkelijk van u kunnen krijgen zodat zij deze gegevens kunnen doorgeven aan een andere organisatie als zij dat wensen. Wist u dat mensen bij de toezichthouder een klacht kunnen indienen over de manier waarop u met hun gegevens omgaat? De toezichthouder is verplicht deze klachten te behandelen..

In de nieuwe privacywetgeving staat de betrokkene centraal: meer mogelijkheden om voor zichzelf op te komen en versterking en uitbreiding van de rechten. Als organisatie is het belangrijk om ervoor te zorgen dat betrokkenen hun rechten goed kunnen uitoefenen.

Ga allereerst binnen uw organisatie na of de huidige procedures voorzien in alle (nieuwe) rechten voor betrokkenen uit de AVG. Deze nieuwe rechten zijn onder meer: recht op informatie, recht van inzage, recht op rectificatie, recht op beperking van de verwerking, recht op overdraagbaarheid (dataportabiliteit), recht van bezwaar en het recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming

(profiling). Sommige van deze rechten stonden ook al in de Wet bescherming persoonsgegevens, anderen zijn nieuw. Hoe start u nu met de inrichting van deze rechten in uw organisatie?

Zorg er eerst voor dat u weet op welke processen de verschillende rechten van invloed zijn. Het recht op inzage heeft bijvoorbeeld invloed op het primaire proces. Immers, de cliënt kan vragen om inzage in het dossier. Als de cliënt vraagt om verwijdering van het dossier heeft dit ook invloed op het primaire proces.

Zorg er vervolgens voor dat betrokkenen hun rechten kunnen uitoefenen. Zorg er voor dat de betrokkenen op een juiste manier worden geïnformeerd over hun rechten. Het meest gebruikte middel om betrokkenen te informeren is via het 'privacystatement' c.q. 'privacyverklaring' op uw website. De informatie moet beknopt worden gegeven, dus geen lang, wollig taalgebruik maar concrete en duidelijk zinnen. Geen juridisch of technisch jargon, maar begrijpelijke taal.

De rechten van betrokkenen zijn niet absoluut. Het feit dat de cliënt zich beroept op het recht op verwijdering betekent niet dat u dat ook altijd moet doen. Volgens bepaalde wetgeving kan het zijn dat u gegevens bijvoorbeeld 5 jaar moet bewaren en u moet dat dan ook doen. Bericht de cliënt dan ook om welke reden (uw wettelijke verplichting) u het verzoek niet kan inwilligen.

De manier waarop de procedures voor de rechten van betrokkenen worden ingericht, is sterk afhankelijk van het type organisatie. Voor zowel grote als kleinere organisaties kan één loket (bijvoorbeeld via een e-mailadres) worden ingericht waar de betrokkenen terecht kunnen.

Artikel 9: Hoe borg ik privacy in de cultuur van de organisatie?

8. Privacycultuur

U wilt privacy borgen doordat privacy door uw medewerkers wordt gedragen. Alleen op die manier zorgt u ervoor dat uw cliënten zo goed mogelijk worden beschermd. Maar, met alleen regels, procedures en afvinklijstjes loopt uw organisatie een groot privacy risico. Immers, zonder het juiste gedrag zijn regels een wassen neus. De grote uitdaging is dan ook om het gedrag in lijn te brengen met deze privacyregels. Dat vraagt om een gezonde privacy cultuur binnen uw organisatie. Welke middelen kunt u inzetten om deze gewenste cultuur positief te beïnvloeden?

Een duurzame verandering is alleen mogelijk als u aandacht besteedt aan de zogenaamde boven- én onderstroom. Een privacy statement, gedragscode en een procedure voor de meldplicht datalekken, de 'bovenstroom', is niet voldoende.

Voorbeeldgedrag van leidinggevenden, vertrouwen en een open cultuur zijn van essentieel belang. Het positief beïnvloeden van de 'onderstroom', de privacy cultuur, vraagt om andere middelen.

Als de boven- en onderstroom in balans zijn, zullen uw medewerkers niet uitsluitend de regels, procedures en afvinklijstjes volgen maar zullen zij handelen in de geest van de wet. Dit is vooral bij de AVG van groot belang omdat de AVG wel aangeeft wat je moet doen, maar niet hoé je dat moet doen. Er zitten veel zogenaamde 'open normen' in de AVG en het is dus aan u om deze zelf in te vullen. Omdat het juridisch kader geen richting geeft, zult u moeten vertrouwen op uw eigen morele kompas.

Het is belangrijk dat u de koppeling maakt tussen beleid en praktijk. Privacy wordt concreet gemaakt voor de medewerkers op de werkvloer. Dit kunt u doen door (een reeks) verschillende acties uit te voeren om aandacht te krijgen voor het onderwerp. Deze acties kunnen variëren van bekers met een privacyboodschap, flyers en posters tot dilemma-sessies, theater en een privacyspel.

Het uiteindelijke doel van deze acties is om de dialoog en het creatieve denkproces over privacy binnen uw organisatie te stimuleren. Het moet in de haarvaten van de medewerkers gaan zitten. Er is hiervoor geen 'one size fits all aanpak' en u zult zelf moeten zoeken naar de passende acties om de privacycultuur positief te beïnvloeden.