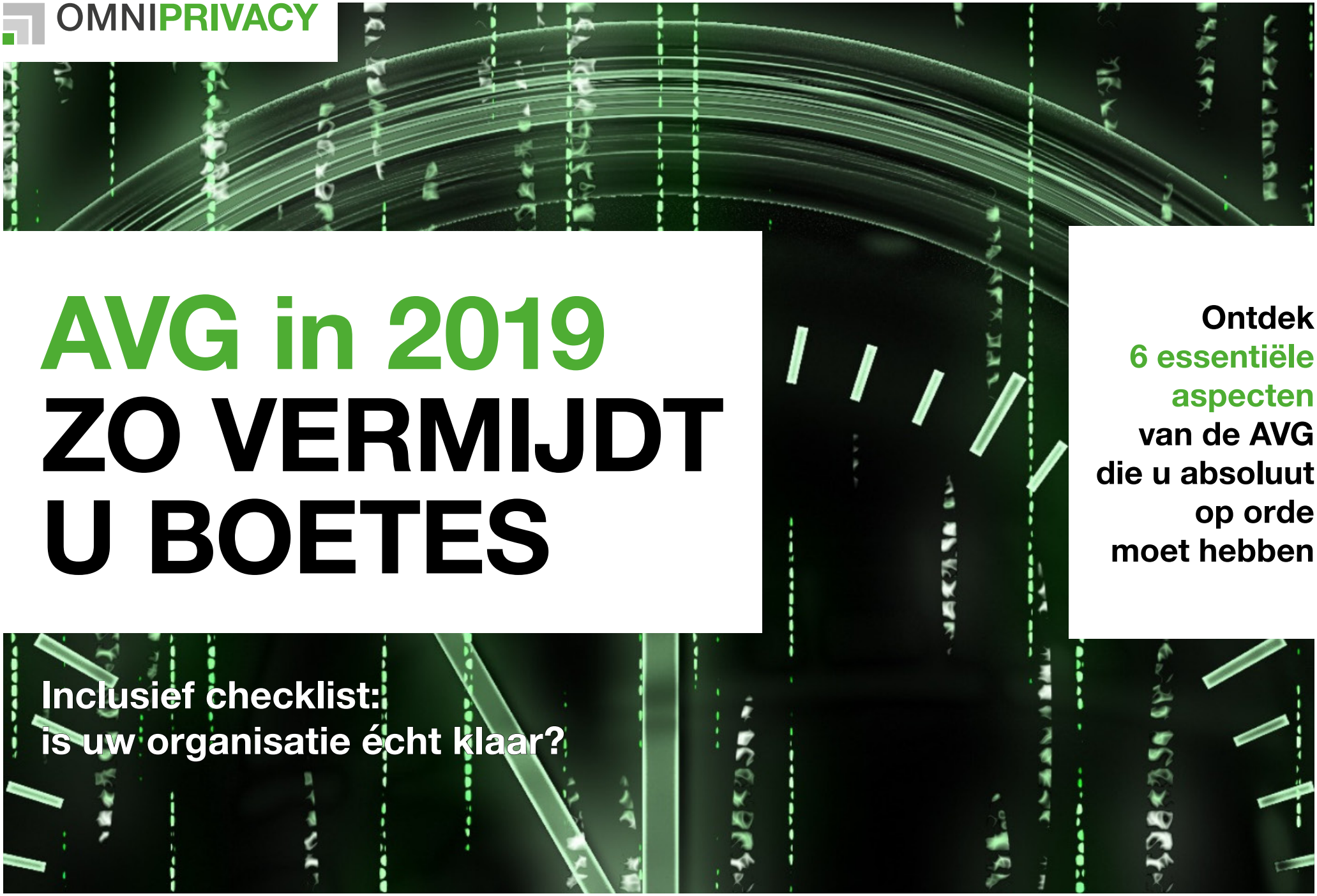
OMNIPRIVACY



AVG in 2019
ZO VERMIJDT U BOETES

Ontdek 6 essentiële aspecten van de AVG die u absoluut op orde moet hebben

**Inclusief checklist:
is uw organisatie écht klaar?**

AVG: de AP gaat nadrukkelijker handhaven

We zijn meer dan één jaar na de invoering van de AVG in Nederland. De nieuwe privacywet bracht inhoudelijk niet veel nieuws ten opzichte van de voorgaande Wet Bescherming Persoonsgegevens. Wat wél veranderde is dat de Autoriteit Persoonsgegevens (AP) nu ook echt zaken kan gaan afdwingen, en daarbij uitgebreide boetebevoegdheid heeft. Sinds 25 mei 2018 kwamen er bij de AP bijna 20.000 privacyklachten binnen. En in de eerste vier maanden van 2019 noteerden ze bijna 8.000 datalekken.

Voor 2019 werd het budget voor de AP (nogmaals) verhoogd, tot 18,5 miljoen euro. Dat moet de AP in staat stellen om nadrukkelijker te gaan handhaven, en sancties op te leggen. Daarnaast zal de AP een systeemtoezicht opzetten, en wil het beter gaan samenwerken met AVG-toezichthouders in andere Europese landen.

Alles wijst er dus op dat de AP vanaf dit jaar meer dan ooit zijn tanden zal laten zien. De enige echte test voor uw AVG-project komt er dus binnenkort aan. En de belangrijkste vraag die u zich vandaag moet stellen, is of uw organisatie écht klaar is voor de AVG.

Waarom u dit e-book moet lezen

Met dit e-book kunt u zich voorbereiden op wat onvermijdelijk gaat komen: controles en boetes van de AP. Het geeft u tips om uw huidige AVG-project te evalueren en eventueel nog bij te sturen. Want de AVG is geen eenmalig project. Het vereist constante aandacht, bijsturing en evaluatie. De kans is bijzonder groot dat de bestaande documentatie die u met het zicht op de AVG samenstelde, reeds verouderd is. Gebruik dit e-book om te zorgen dat uw organisatie of bedrijf sterk in de schoenen staat bij een controle of vraag van de AP.

Bent u Functionaris Gegevensbescherming dan kunt u met dit e-book het AVG-topic terug ter sprake brengen bij het management. Bent u manager, dan biedt dit e-book een snelle manier om te evalueren of er toch nog een domein is dat bijsturing kan gebruiken of een update nodig heeft.

leestijd:
12 minuten

“Binnenkort gaan we optreden, en daarvan verwacht ik dat mensen gaan zeggen: Dat snap ik wel, het is goed dat de AP daartegen optreedt”

Aleid Wolfsen, voorzitter Autoriteit Persoonsgegevens, in een interview met Tweakers (juni 2019)

Ik bezit een up-to-date overzicht van alle persoonsgegevens die ik verwerk

WAT ZEGT DE WET?

De **AVG** verwacht dat u een dataregister aanlegt. Daarin documenteert u gedetailleerd welke persoonsgegevens u opslaat, waar en hoe u ze verwerkt en beschermt, en met wie u deze gegevens eventueel deelt.

Het dataregister - of ook: register van de verwerkingsactiviteiten - is het eerste document dat de Autoriteit Persoonsgegevens (AP) bij een controle zal opvragen. Een compleet en up-to-date dataregister is zonder twijfel het beste bewijs dat u uw huiswerk goed heeft gemaakt. Heeft uw organisatie minder dan 250 werknemers, dan is een dataregister niet altijd verplicht, al raadt de AP wel aan om er een op te stellen.

HOE PAKT U HET AAN?

U moet eerst grondig onderzoek doen om een volledig beeld te krijgen van de verwerking van gegevens, en dit zowel binnen als buiten uw organisatie. Een eenvoudig Excel-bestand is voor veel organisaties de meest voor de hand liggende manier om hun dataregister samen te stellen. En volgens de AVG is zo'n overzicht in Excel perfect toegelaten. Echter, liefst 20 procent van de (meta)data is al na amper één jaar verouderd. Uw grootste uitdaging is dan ook om de vele wijzigingen die nog staan te gebeuren, zo snel mogelijk te laten doorstromen naar het dataregister. Dat dit doorstromen geïnitieerd moet worden door verschillende mensen en vanuit alle afdelingen, maakt de uitdaging extra complex.

VOORBEELDEN

1 Uw verkopers hebben een nieuw (en mogelijk gevoelig) **informatieveld** toegevoegd aan de CRM-applicatie voor klanten- en prospectenopvolging

2 U boekt een teamevent en moet de **adresgegevens** van alle deelnemers doorgeven

3 Een nieuwe **back-uptool** bewaart bestanden in de cloud bij een Amerikaanse provider

"Liefst 20 procent van de (meta)data is al na amper één jaar verouderd"

ADVIES

Controleer regelmatig of uw dataregister nog wel een accuraat beeld schetst van de werkelijke situatie inzake gegevensverwerking binnen uw organisatie. Maak daarnaast alle medewerkers en afdelingen ervan bewust dat ze wijzigingen met betrekking tot de opslag van persoonsgegevens, hoe klein ook, altijd moeten doorspelen aan de persoon die verantwoordelijk is voor het dataregister.

Ik kan een datalek tijdig melden en opvolgen (ook in het weekend)

WAT ZEGT DE WET?

Uiteraard heeft u op voorhand de **veiligheidsrisico's** in kaart gebracht (zie pagina 7) en doet u er alles aan om de beveiliging van persoonsgegevens te maximaliseren. Indien u toch een verlies van data opmerkt, dan moet u dit binnen de 72 uur melden aan de AP.

Er zijn wel enkele uitzonderingen, bijvoorbeeld wanneer de verloren gegevens voldoende versleuteld zijn. Uiteindelijk ligt de beslissing om een datalek al dan niet te melden bij uw management, dat daarbij wordt bijgestaan door de Functionaris Gegevensbescherming (FG).

HOE PAKT U HET AAN?

De AP voorziet in een **online procedure** om datalekken te melden. Een grote misvatting is dat wanneer u een datalek meldt bij de AP, u sowieso een boete of controle mag verwachten. Anderzijds: als u jarenlang géén datalek zou melden, dan is de kans groot dat u vanzelf op de radar van de AP komt. U contacteert en informeert ook alle betrokkenen van wie de data geïmpacteerd zijn, en uiteraard volgt u de zaak verder op. Daarnaast is het belangrijk dat u kunt aantonen wat u allemaal gedaan heeft om dit lek niet alleen correct af te handelen maar ook om het te voorkomen. Een goed onderbouwde verantwoording zal u helpen om eventuele boetes te vermijden.

VOORBEELDEN

1. U stuurt per ongeluk een e-mail of brief naar de verkeerde persoon
2. De laptop van een medewerker wordt gestolen
3. Een usb-stick raakt verloren
4. Een hacker verkrijgt toegang tot de cloudopslag van een medewerker

Doet u een beroep op een externe partij voor uw gegevensverwerking, of verwerkt u zelf gegevens van andere organisaties? Dan moet in de verwerkingsovereenkomst met die partijen beschreven staan hoe een gegevenslek gemeld moet worden.

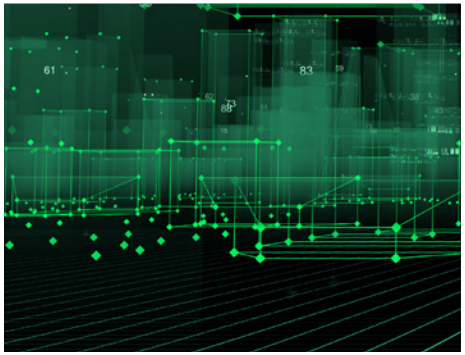
ADVIES

Snel kunnen beslissen en vervolgens uitvoeren is cruciaal bij een datalek. Dit vergt doordachte interne én externe communicatie. Maak iemand verantwoordelijk voor deze taak - meestal de FG - en voorzie ook permanentie in weekends en tijdens feestdagen.

Ik kan tijdig voldoen aan privacyverzoeken van medewerkers, klanten enzovoort

WAT ZEGT DE WET?

Iedereen van wie u persoonsgegevens verwerkt, heeft in principe het recht om deze in te zien, op te vragen of te laten schrappen. Dit laatste valt onder het zogenaamde **'recht om vergeten te worden'**. U moet een afdoende antwoord kunnen geven op dit soort vragen, en dit binnen een periode van 30 dagen. Al kunt u wel tot tweemaal toe uitstel vragen met eenzelfde termijn.



HOE PAKT U HET AAN?

Een **privacyverzoek** kan op verschillende manieren binnenkomen in uw organisatie. Via de klantendienst, via de IT-helpdesk, via een speciaal portaal dat u hiervoor heeft voorzien, of zelfs direct via de verantwoordelijke voor gegevensverwerking. Vergeet ook niet dat externe partijen waarmee u verwerkingsovereenkomsten heeft afgesloten, een bron kunnen zijn voor dit soort aanvragen. Dit laatste scenario is zelfs het meest waarschijnlijke. Vervolgens start een proces dat gelijkenissen vertoont met de melding van een datalek (zie pagina 4).

VOORBEELDEN

1 U krijgt een **brief of e-mail** met daarin het verzoek om persoonlijke gegevens te wissen

2 Een **nieuwsbriefabonnee** wens zich uit te schrijven of zijn e-mailadres aan te passen

3 Een **werknemer verlaat het bedrijf** en wil weten welke informatie u over hem of haar bijhoudt

ADVIES

In grotere organisaties is een snelle detectie van het privacyverzoek van groot belang. Zorg dat binnen elk departement de rol van *data-owner* bekend is, zodat u tijdig een antwoord kunt sturen.

Denk ook aan ...

Heldere communicatie speelt een belangrijke rol bij de AVG. U kunt er zich niet vanaf maken met wollige omschrijvingen en onduidelijke formuleringen om van privépersonen toestemming te krijgen om hun persoonsgegevens bij te houden en te verwerken. Daarnaast moet u steeds de juiste grondslag kennen (zie kaderstukje) op basis waarvan u gegevens mag verwerken.

U mag persoonsgegevens enkel verwerken indien ...

1. u toestemming heeft van de betrokkene
2. dit noodzakelijk is voor de uitvoering van een overeenkomst
3. u moet voldoen aan een wettelijke verplichting
4. u de vitale belangen van de betrokkene moet beschermen
5. dit nodig is in het belang van de werking van uw organisatie
6. het om een taak van algemeen belang gaat

Mijn privacyverklaring is correct opgesteld en up-to-date

De privacyverklaring vormt de basis om uw (online) dataverwerking te duiden bij prospecten, betrokkenen en de buitenwereld in het algemeen. Het is dus een belangrijk document. Het is niet alleen nodig volgens de AVG; een duidelijke en complete omschrijving van hoe u privacy aanpakt zal ook meer vertrouwen geven aan de websitebezoeker.
De privacyverklaring is onderhevig aan regelmatige veranderingen en dus moet u ze beschouwen als een dynamisch document.

Versiebeheer zal u helpen om steeds de meest recente tekst te kunnen tonen, niet alleen op uw website, maar ook op andere plaatsen waar u met de buitenwereld communiceert.

TIP: wees transparant, en stel een privacyverklaring op die compleet is en eenvoudige taal gebruikt. Zorg dat overal in uw organisatie de laatste versie gebruikt wordt.

Ik kan bewijzen dat ik toestemming heb om klanten en prospects te contacteren

Het is de essentie van de AVG: u moet voortaan goede redenen hebben om persoonsgegevens te verwerken. Bovendien moet u, wanneer het om toestemming gaat, kunnen aantonen waar en wanneer die toestemming gegeven is, en in welke omstandigheden. Een toestemming is bijvoorbeeld ongeldig als ze verkregen is op een manier waarbij er geen vrijheid van keuze was. Voorbeeld: u geeft enkel toegang tot de blog op uw website als men zich ook inschrijft op uw nieuwsbrief.

TIP: ga vooraleer u iemand contacteert, bijvoorbeeld via een mailing, na of u daarvoor (nog steeds) de toestemming heeft en zorg dat u dit ook kunt staven. Streef de zogenaamde *golden consent* na, de meest complete en meest recente registratie van de toestemming.

Ik schat de risico's van gegevensverwerking correct in

WAT ZEGT DE WET?

Indien u gevoelige persoonsgegevens verwerkt, dan moet u de risico's die daarmee gepaard gaan in kaart brengen door middel van een **Gegevensbeschermings-effectbeoordeling** (GEB), ook wel DPIA genoemd. Niet alleen de risico's van dergelijke gegevensverwerking, maar ook de bijhorende maatregelen dienen in de GEB gedocumenteerd te worden.

Volgens de Autoriteit Persoonsgegevens (AP) is een GEB verplicht als u aan 'uitgebreide profilering' doet, of bij een 'grootschalige verwerking van bijzondere categorieën van gegevens', en dit ongeacht de bedrijfsgrootte.

HOE PAKT U HET AAN?

Het **dataregister** (zie pagina 3) zal de richting bepalen voor de rapportering van de GEB. Maar hoe u een GEB aanpakt, bepaalt u zelf. Betrek bij de risico-inschatting alle betrokken partijen binnen het bedrijf of de organisatie, inclusief de interne gebruikers van de gegevens. Moest uit de GEB blijken dat uw verwerkingen zonder het nemen van maatregelen tot een hoog risico leiden, dan moet het rapport voorgelegd worden aan de Autoriteit Persoonsgegevens zodat deze advies kan geven.

VOORBEELDEN

1 U verwerkt gevoelige gegevens zoals etnische afkomst of politieke voorkeuren

2 U haalt op grote schaal gegevens binnen die gegenereerd worden door Internet of Things-toepassingen

3 Uw bewakingscamera's registreren activiteiten in openbare ruimten

4 U houdt uitgebreide gegevens bij van uw klanten om ze te profileren voor marketing- en verkoopscampagnes

ADVIES

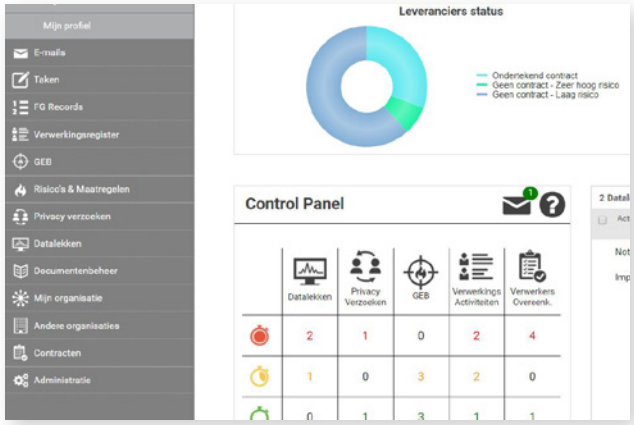
Een GEB is enkel in specifieke gevallen verplicht. Toch raden we u aan om dit sowieso te doen. Het biedt namelijk een uitgelezen kans om een scherpe kijk op privacy te behouden, en in het bijzonder op de risico's die overal in uw organisatie aanwezig zijn. U stelt zo gerichter prioriteiten op, op basis waarvan u dan aangepaste (beveiligings)budgetten kunt toekennen. Net zoals bij het dataregister is een regelmatige update van de GEB aan te raden, minstens om de twee jaar.

√ Checklist

- ☐ Ik bezit een up-to-date overzicht van alle persoonsgegevens die ik verwerk
- ☐ Ik kan een datalek tijdig melden en opvolgen (ook in het weekend)
- ☐ Ik kan tijdig voldoen aan privacyverzoeken van klanten, medewerkers enzovoort
- ☐ Mijn privacyverklaring is correct opgesteld en up-to-date
- ☐ Ik kan bewijzen dat ik toestemming heb om klanten en prospects te contacteren
- ☐ Ik schat de risico's van gegevensverwerking correct in

AVG op de werkvloer: naar een methodische aanpak

Hoeveel items in de checklist heeft u afgevinkt? Alle zes? Proficiat! Dan kunt u met een gerust hart een bezoek of controle doorstaan. In alle andere gevallen herevalueert u best uw AVG-project. Een methodische aanpak werkt het best, maar Excel is daarvoor niet de aangewezen tool. Er bestaan gelukkig hulpmiddelen die u op een volledig geïntegreerde manier helpen om continu AVG-compliancy na te streven. Benieuwd hoe dergelijke tools werken? **Volg dan ons gratis webinar via de knop hiernaast.**



Met een tool zoals Omniprivacy krijgt u een volledig zicht op uw AVG-compliancy

GRATIS WEBINAR

Met **OMNIPRIVACY** naar een methodische AVG-aanpak met behulp van een geïntegreerde tool.

INFO & DATA

https://click.omniprivacy.be/yws

OMNIPRIVACY NEDERLAND
President Kennedylaan 19
2517 JK Den Haag (NL)
+31 (70) 711 8380
sales@omninet.nl