contrast

UW BUSINESS • MEI 2021

De AVG in (een checklist van) 10 punten? Ja, dat kan!

Wat u moet weten.

De AVG trad in werking precies 3 jaar geleden, op 25 mei 2018. Heel wat ondernemingen zijn rond die periode gestart met de implementatie van de AVG, maar zien ondertussen door het bos de bomen niet meer. Andere ondernemingen weten überhaupt niet waar te beginnen. En die ondernemingen die de oefening ooit hebben afgerond, zinkt de moed in de schoenen als ze denken aan een evaluatie en update van de eerste oefening.

Is dit een overdrijving? Zeker niet! De 88 pagina's AVG telt 55.000 woorden, opgenomen in 173 overwegingen en 99 artikelen. Hieruit (alle) concrete verplichtingen identificeren is geen eenvoudige taak. Maar er zijn hulpmiddelen!

Verschillende nationale gegevensbeschermingsautoriteiten hebben al heel wat nuttige instrumenten gepubliceerd: van GDPR stappenplannen (bijvoorbeeld van de Franse CNIL) tot concrete modellen (bijvoorbeeld de verwerkersovereenkomst van de Deense Datatilsynet). Het is dus zeker nuttig om de websites van de autoriteiten te raadplegen. Toch ontbreekt nog een volledig, en tegelijkertijd beknopt en echt praktisch, overzicht dat toelaat om systematisch alle verplichtingen onder de AVG te checken. **contrast** heeft daarom een checklist opgesteld met 10 punten.

Wat u moet doen.

Als uw onderneming de AVG (nog) niet onder de knie heeft, weet dan dat zij zeker niet alleen is! Het is niet te laat om de AVG oefening op te starten, verder te zetten of up te daten. Het is evenmin een onmogelijke opdracht. Bij **contrast** gebruiken we de volgende 10 punten checklist:

1. **Doel**: start met het identificeren van de verschillende doeleinden waarvoor uw onderneming persoonsgegevens verwerkt. Leg deze vraag bij de verschillende departementen binnen uw onderneming: HR, verkoop, marketing, enz. U kan hen alvast wat inspiratie geven door vaak

voorkomende verwerkingsdoeleinden (met een concrete omschrijving) mee te geven. Op basis van deze doeleinden, bepaalt uw onderneming welke persoonsgegevens noodzakelijk zijn en hoelang uw onderneming ze mag bewaren.

2. **Grondslag**: identificeer voor elk van de doeleinden de meest gepaste wettelijke grondslag conform artikel 6 tot en met 10 AVG. Dit is een taak voor juristen in overleg met de medewerkers die binnen uw onderneming verantwoordelijk zijn voor de verwerking. In functie van de gekozen grondslag (toestemming, gerechtvaardigd belang, enz.) zullen mogelijk bijkomende acties nodig zijn.

3. **Rechten**: ga na of de geïdentificeerde doeleinden (en alle daarmee verbonden informatie conform artikel 13 en 14 AVG) zijn opgenomen in een privacyverklaring voor de betrokkenen. Verwerkt uw onderneming persoonsgegevens via haar website? Dan is een privacyverklaring op de website noodzakelijk. Beslist uw onderneming om een lijst met verjaardagen van haar werknemers op te stellen om verjaardagswensen te versturen? Dan moet u checken of dit is opgenomen in de privacyverklaring voor werknemers. Verder is het belangrijk om procedures te voorzien voor het beantwoorden van verzoeken van betrokkenen in overeenstemming met onder meer artikel 12 AVG: is een absolute opt-out voor direct marketing voorzien, wie zal een verzoek om inzage beantwoorden, hoe moet een betrokkene zijn identiteit bewijzen, welke (antwoord)modellen moeten gebruikt worden,enz.?

4. **3e partijen**: identificeer voor elk van de doeleinden de derde partijen die toegang hebben tot / gebruik maken van de persoonsgegevens. Laat een jurist helpen bij de kwalificatie van deze derde partijen als verwerker, gezamenlijke verwerkingsverantwoordelijke of afzonderlijke verwerkingsverantwoordelijke. Verlies ook groepsondernemingen niet uit het oog! In functie van die kwalificatie moet u verifiëren of de nodige (contractuele) documenten voorhanden zijn.

5. **3e landen**: ga na of deze 3e partijen zich buiten de Europese Economische Ruimte bevinden of zij een dochteronderneming zijn waarvan de moedervennootschap zich buiten de EER bevindt. Indien dat het geval is, moet uw onderneming de nodige waarborgen treffen om een gelijkwaardig beschermingsniveau in het desbetreffende 3e land te garanderen. Ook hierbij kunnen juristen helpen.

6. **Beveiliging en datalekken**: ga in functie van de risico’s die gepaard gaan met de verwerking na of de huidige beveiliging / welke beveiliging passend is om de persoonsgegevens te beschermen tegen ongeoorloofde toegang, verlies en wijziging. De risico’s (en dus te nemen maatregelen) zullen afhankelijk zijn van de types persoonsgegevens die verwerkt worden, welke technologieën en infrastructuur gebruikt worden in het kader van de verwerking, etc. Het is aangewezen om hier beroep te doen op (IT) beveiligingsconsulenten. Het zal niet mogelijk zijn om elk risico volledig uit te sluiten. Daarom is het belangrijk dat uw onderneming ook maatregelen treft om datalekken te identificeren, intern te documenteren en te melden aan de bevoegde autoriteit en betrokkenen.

7. **DPO**: verifieer of (één of meerdere van) de doeleinden ertoe leiden dat u als onderneming een

data protection officer moet aanstellen en melden bij de bevoegde gegevensbeschermingsautoriteit(en).

8. **DPIA**: verifieer of (één of meerdere van) de doeleinden gepaard gaan met een hoog risico voor de betrokkenen. Deze analyse kan u onder meer doen op basis van de lijsten die de gegevensbeschermingsautoriteiten hebben gepubliceerd of aan de hand van de criteria van het Europees Comité voor Gegevensbescherming. In geval van een hoog risico, moet u een gegevensbeschermingseffectbeoordeling (een soort van impact analyse) doen en eventueel voorafgaande goedkeuring van de bevoegde gegevensbeschermingsautoriteit vragen.

9. **Policies en procedures**: zorg ervoor – ook indien uw onderneming niet verplicht is om een DPO aan te stellen – dat er *minstens iemand* centraal verantwoordelijk is voor de opvolging van de naleving van de AVG binnen uw onderneming. Zorg ook voor bewustmaking en opleiding van uw personeel. Verder moet elke onderneming in elk geval een procedure hebben voor het beantwoorden van verzoeken van betrokkenen, voor het documenteren en melden van datalekken, voor het verwijderen van persoonsgegevens en voor de correcte beveiliging van persoonsgegevens (bijvoorbeeld per datasysteem). Het register (zie hieronder) kan hiervoor een nuttig instrument zijn. Het is ook nuttig om bijvoorbeeld het gebruik van deze checklist op te nemen in de standaardprocedures voor het opstarten van nieuwe projecten.

10. **Register**: zorg ervoor dat de informatie die verzameld wordt in het kader van deze checklist wordt opgenomen in een register voor verwerkingsactiviteiten conform artikel 30 AVG.