



AVG-ondersteuning bij uw klant



Oktober 2018

© 2018 Koninklijke NBA

Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij door middel van druk, fotokopieën, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van de NBA.

Disclaimer

Deze brochure is zo zorgvuldig mogelijk samengesteld. De NBA is echter niet aansprakelijk voor eventuele onjuistheden. De NBA heeft er voor gekozen een maximaal leesbare brochure op te stellen.

Oktober 2018

AVG-ondersteuning bij uw klant

De Algemene Verordening Gegevensbescherming (AVG) stelt niet alleen eisen aan accountantskantoren maar aan alle ondernemingen, verenigingen, stichtingen etc. die persoonsgegevens verwerken. Als accountant heeft u zich voor uw eigen kantoor moeten verdiepen in de AVG-eisen en de gevolgen voor de praktijk. Mogelijk heeft u, of een collega, cursussen of opleidingen gevolgd. Van de NBA kreeg u onder meer ondersteuning door het aanbieden van modelovereenkomsten (zie; www.nba.nl/tools-en-voorbeelden/model-bewerks-overeenkomst/) en de privacytoolkit (zie: www.mijnnba.nl/avg/).

De opgebouwde kennis is natuurlijk niet alleen voor uw eigen kantoor te gebruiken, maar mogelijk ook in te zetten voor klanten. Vrijwel iedere klant zal immers met de AVG te maken hebben, terwijl niet alle organisaties al aan de AVG vereisten voldoen.

Uw rol als Trusted Advisor kan per klant verschillen. Zo zal een doorsnee MKB-bedrijf vaak beperkt persoonsgegevens verwerken. Waarschijnlijk kunt u deze klant vrijwel compleet AVG-proof helpen maken. Indien de klant veel persoonsgegevens verzamelt en bewaart binnen een geautomatiseerde omgeving, zoals bijvoorbeeld bij een webshop met particuliere afnemers, zal uw rol mogelijk meer ondersteunend zijn en zullen er andere specialisten worden ingeschakeld.

Hieronder beschrijven we kort enkele aandachtspunten in een stappenplan dat u kunt gebruiken bij het adviseren van uw klant.

Nul-meting

Door uw kennis van de onderneming van de klant, aangevuld met interviews met het bestuur/ de eigenaar van de onderneming en eventuele werknemers van het bedrijf, kunt u erachter komen of er, naast de eventueel door u gevoerde (salaris) administratie, persoonsgegevens worden verwerkt. Op de site **mijn NBA** vindt u diverse downloads die u kunnen helpen. www.mijnnba.nl/avg/downloads/

Vragen die kunnen opkomen zijn bijvoorbeeld (niet uitputtend);

- Is er een overzicht van de verwerkingen?
- Zijn er evt. verwerkersovereenkomsten?
- Zijn alle medewerkers bij de klant bewust van de gevolgen van de AVG?
- Worden er bijzondere categorieën van persoonsgegevens verwerkt, zoals bijvoorbeeld medische gegevens? Aan deze verwerking worden strengere eisen gesteld.
- Is er een geldige grondslag? Bijvoorbeeld uitvoeringsovereenkomst, wettelijke verplichting of toestemming.
- Is er een procedure voor de rechten van betrokkenen? (inzage, etc.)
- Worden er niet meer persoonsgegevens verwerkt dan strikt noodzakelijk? En ook niet langer dan noodzakelijk?
- Is er een passend beveiligingsniveau? Mogelijk kan de ICT checklist hierbij helpen; www.nba.nl/avg-basischecklist-automatisering/
- Is er specifieke (zelf ontworpen) software zodat er een Data Protection Impact Assessment (DPIA) nodig is?
- Is er een passende privacyverklaring op de website

- Is er een functionaris voor de gegevensbescherming vereist, en zo ja, aanwezig?
- Is er voldoende aandacht voor datalekken? (procedure, instructies, register)
- Bij een internationaal bedrijf; wie is de leidende toezichthouder?

Projectplan

Nadat u de stand van zaken in kaart heeft gebracht, is de volgende stap het opstellen van een projectplan. U kunt hierbij de klant helpen om beslissingen te nemen over de aanpak en de eventuele inschakeling van specialisten. Zeker wanneer de klant sterk afhankelijk is van het geautomatiseerd op grote schaal verwerken van persoonsgegevens, is de inschakeling van externe specialisten al snel aan de orde.

Door uw kantoor of derden uit te voeren werkzaamheden kunnen o.a. zijn;

- Het inventariseren van verwerkingen ten behoeve van het opzetten van een verwerkingsoverzicht.
- Het beoordelen en adviseren van de beveiligingsmaatregelen.
- Het opzetten van een datalekprocedure en datalekregister.
- Het opzetten of beoordelen van een privacyverklaring t.b.v de website van de klant.
- Het beoordelen of opstellen van verwerkingsovereenkomsten.

Daarnaast kunnen er, bijvoorbeeld wanneer er sprake is van complexe privacyaspecten of er meer zekerheid gewenst is, specialisten worden ingeschakeld voor;

- Data Protection Impact Assessment (DPIA); hierbij worden de privacyaspecten van een gegevensverwerking vooraf in kaart gebracht. (van belang wanneer er bijvoorbeeld maatwerk software wordt geïnstalleerd waarbij persoonsgegevens worden verwerkt)
- Penetratietest (pentest); dit betreft een kwetsbaarheidsonderzoek inzake de website en de achterliggende systemen. Dit kan defensief (systeembeoordeling) of offensief (met hackers) gebeuren.
- Het verkrijgen van het keurmerk 'Privacy-Audit-Proof'. Hiervoor is bijvoorbeeld door NOREA (beroepsorganisatie van IT-auditors) een Privacy Control Framework ontwikkeld.

Het is van belang om in het projectplan een tijdlijn op te nemen en deze gedurende de implementatie te bewaken.

Implementatie

Afhankelijk van de actiepunten in het projectplan en wie deze gaat uitvoeren, kunt u aan de slag met de nodige werkzaamheden, dan wel de klant ondersteunen bij het volgen van de door derden uit te voeren werkzaamheden.

Door regelmatig met de klant in gesprek te gaan, kunt u ertoe bijdragen dat de tijdlijn gevolgd wordt en de implementatie volgens planning plaatsvindt.

Toetsing (1-meting)

Na de implementatiefase is het zaak om nog een keer te toetsen of nu alle relevante punten geraakt zijn. Hiertoe kunt u de onderdelen van de 0-meting die nog niet in orde waren, nog een keer bezien, zodat duidelijk is of de klant nu aan de AVG voldoet. Daarnaast is het van belang dat de klant haar medewerkers op de hoogte houdt over nieuwe procedures en maatregelen als gevolg van de AVG, zodat naleving hiermee grotendeels wordt geborgd.

Tenslotte is het zaak om bij wijzigingen van de AVG of wijzigingen in de activiteiten van de klant, steeds aandacht te hebben voor de AVG-aspecten bij de klant. Dit zou een vast onderwerp bij de jaarrekening bespreking met de klant kunnen zijn.

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants



Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl