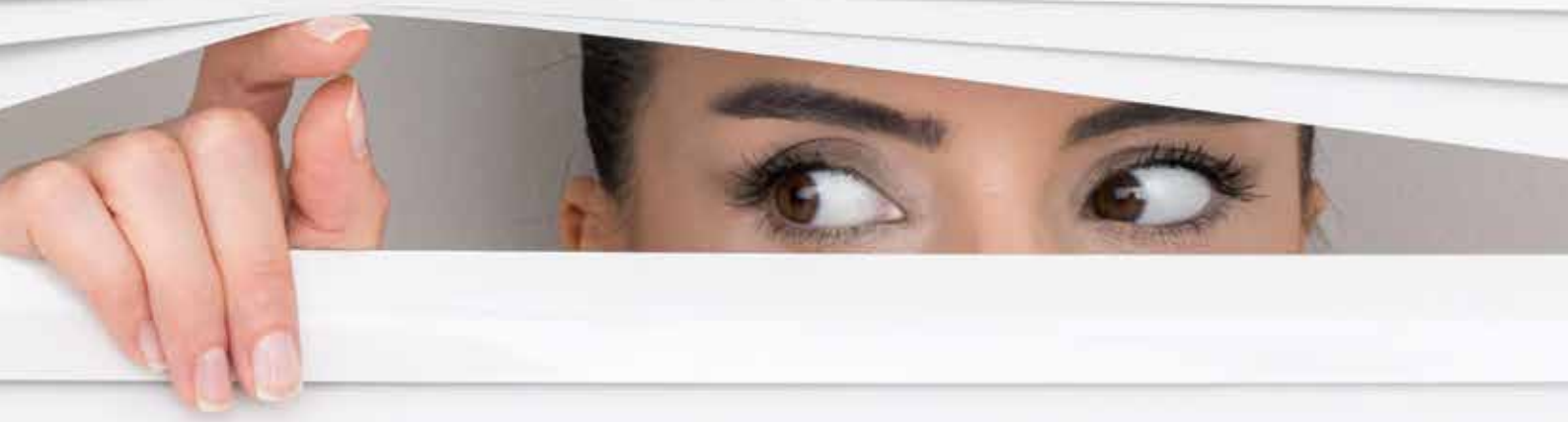
Algemene Verordening Gegevensbescherming

AVG en uw organisatie



Aan de slag!

- Leg vast waar en met welk doel u binnen uw organisatie persoonsgegevens verwerkt, en welke verwerkingen dat zijn.
- Sluit verwerkers-overeenkomsten met uw leveranciers en laat deze beoordelen.
- Creëer intern bewustwording. Informeer uw medewerkers en leg privacy spelregels vast.
- Doe aan dataminimalisatie: verzamel alleen de persoonsgegevens die u daadwerkelijk nodig hebt.
- Beoordeel of uw ICT-systemen voldoende beveiligd zijn.

Hoek en Blok
accountants | belastingadviseurs | juristen

Rust en ruimte om te ondernemen

Wat zijn de basis AVG-vereisten voor uw organisatie?

Per 25 mei 2018 is in Nederland de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De AVG zorgt ervoor dat persoonsgegevens in de gehele EU dezelfde bescherming krijgen, dus ook in Nederland. Bedrijven die persoonsgegevens verwerken dienen zich steeds weer de vraag te stellen of de verwerking in lijn is met de regels; regels die zijn gebaseerd op een aantal solide en algemeen geaccepteerde privacy beginselen. De AVG in tien punten.

1 Verwerk ik persoonsgegevens?

Gaat u daar maar van uit! Als u informatie (waaronder NAW-gegevens, geboortedata, salarisgegevens, BSN-nummers) verzamelt, vastlegt, opslaat, bijwerkt, opvraagt, raadpleegt of gebruikt aan de hand waarvan een natuurlijk persoon kan worden geïdentificeerd (direct dan wel indirect), dan verwerkt u persoonsgegevens.

2 Waar kom ik persoonsgegevens tegen in mijn organisatie?

U vindt persoonsgegevens op diverse plaatsen binnen uw onderneming. Gaat u maar eens na. U bewaart en verzamelt persoonsgegevens voor zowel interne doeleinden zoals personeelsdossiers en gegevens van sollicitanten. Ook voor externe doeleinden, zoals bijvoorbeeld marketing of verzending van producten.

3 Mag ik persoonsgegevens verwerken?

De AVG noemt een aantal gronden op basis waarvan u persoonsgegevens mag verwerken. De meest voorkomende zijn: toestemming van de betrokkene, noodzakelijkheid voor de uitvoering van een overeenkomst, het voldoen aan een wettelijke verplichting en/of de aanwezigheid van een gerechtvaardigd belang. Dat laatste moet u overigens wel goed kunnen onderbouwen. Het enkel hebben van toestemming is overigens niet voldoende. U dient deze toestemming te allen tijde aan te kunnen tonen. Ga daar dus zorgvuldig mee om.

4 Verwerk ik op de juiste manier?

U dient persoonsgegevens te verwerken op rechtmatige, behoorlijke en transparante wijze. Persoonsgegevens mogen enkel worden verzameld voor een uitdrukkelijk omschreven en gerechtvaardigd doel (doelbinding) én de hoeveelheid te verzamelen persoonsgegevens dient te worden beperkt tot wat noodzakelijk is voor het bereiken van dat doel. Dataminimalisatie heet dat met een mooi woord. Bezit u bijvoorbeeld iemands persoonsgegevens teneinde hem/haar een product te kunnen leveren, gebruik deze dan niet om hem/haar te bestoken met reclamefolders. Tenzij u daarvoor toestemming hebt.

5 Wat zijn de rechten van betrokkenen?

Iedere betrokkene heeft het recht om vergeten te worden (het recht op vergetelheid). Iedere persoon wiens persoonsgegevens door u worden verwerkt, kan u dan ook verzoeken om de door u verwerkte persoonsgegevens in te zien, aan te vullen, daaraan correcties aan te brengen en/of deze te verwijderen. Een eerder verleende toestemming kan door een betrokkene bovendien weer worden ingetrokken. U dient aan een verzoek van een betrokkene binnen vier weken te voldoen. Let op: weg is weg. Gegevens dienen dus ook uit archieven en eventuele back-ups te worden verwijderd.

6 Maak ik bij de verwerking gebruik van de hulp/diensten van derden?

U dient in kaart te brengen of u bij het verwerken van persoonsgegevens gebruik maakt van de diensten van derden, zogenoemde verwerkers. Uw softwareleverancier kan een verwerker zijn in de zin van de AVG, net als de partij die uw salarisadministratie verzorgt. U dient met hen een verwerkersovereenkomst te sluiten waarin wordt geregeld dat de verwerker de persoonsgegevens verwerkt conform de AVG en hierbij passende technische en organisatorische maatregelen treft teneinde de persoonsgegevens te beschermen. Houd er rekening mee dat u verantwoordelijk blijft voor de verwerking van de persoonsgegevens. U dient dan ook periodiek te monitoren of de door u ingeschakelde verwerker nog voldoet aan de vereisten van de AVG.

7 Een datalek, wat nu?

Zijn er persoonsgegevens verloren gegaan of aangetast en/of heeft een onbevoegde derde toegang gehad tot uw gegevens? Neem dan adequate maatregelen. Een datalek is erg vervelend, belangrijker nog is hoe u erop anticipeert. Beoordeel allereerst of daadwerkelijk

sprake is van een datalek. Als u bijvoorbeeld over een back-up beschikt, dan zijn er geen persoonsgegevens verloren gegaan en is in beginsel geen sprake van een datalek. En als u kunt uitsluiten dat een onbevoegde-derde gegevens heeft aangetast of vervreemd, is evenmin sprake van een datalek. Mocht er wel sprake van zijn een datalek, beoordeel dan of dit datalek moet worden gemeld aan de Autoriteit Persoonsgegevens en/of de betrokkene.

8 Bewaartermijnen

U mag persoonsgegevens niet langer bewaren dan strikt noodzakelijk is voor het bereiken van het beoogde doel. Bepaalde gegevens dienen vanwege administratieve redenen en/of wettelijke voorschriften voor een langere periode te worden bewaard, maar zodra deze termijnen zijn verlopen dient algehele verwijdering van de betreffende persoonsgegevens plaats te vinden. Houd er ook rekening mee dat gegevens van sollicitanten niet mogen worden bewaard, tenzij daar toestemming voor is gegeven. En dan nog is een bewaartermijn van één jaar het maximum.

Bewaartermijnen in de praktijk

Ziekte 2 jaar na afronden ziekteverzuim-perioden of afsluiten re-integratie dienen de dossiers uit het personeels-dossier verwijderd te worden.	**Loonadministratie** 2 jaar na einde dienstverband tenzij een wettelijke bewaarplicht geldt.
Personeelsadministratie 2 jaar na einde dienstverband.	**Klantcontactgegevens** 1 jaar (in beginsel) nadat de relatie is verbroken.
Interne telefoon- en adressenlijst 6 maanden nadat de persoon uit dienst is getreden.	**Debiteuren en crediteuren** 2 jaar nadat de vordering is voldaan.

9 Wat moet ik allemaal regelen?

Breng allereerst in kaart (of laat dat doen) of u persoons-gegevens verwerkt, waar u ze binnen uw organisatie verwerkt, of u ze mag verwerken en zo ja, of u dat op juiste wijze doet. Sluit verwerkersovereenkomsten met uw verwerkers, zorg voor protocollen ten aanzien van de rechten van betrokkenen en datalekken en leg een datalekregister aan waarin incidenten worden geregistreerd. De AVG verwacht van u dat u passende technische en organisatorische maatregelen treft, teneinde door u verwerkte persoonsgegevens te beschermen. Kweek bewustwording onder uw personeel. Laat hen informatie op USB-sticks versleutelen, zorg ervoor dat laptops niet in auto's rondslingeren, laat hen niet nodeloos persoons-gegevens opslaan in uw systemen en wees zorgvuldig bij bijvoorbeeld het e-mailen van persoonsgegevens. Wijs tenslotte iemand binnen uw organisatie aan die verantwoordelijkheid krijgt en het aanspreekpunt is voor het privacyvraagstuk binnen uw organisatie.

10 Dienstverlening Hoek en Blok

Documentatie

Hoek en Blok beschikt over diverse modellen die in het kader van de AVG benodigd zijn, zoals: een register van verwerkingen, verwerkersovereenkomst, privacy-verklaring en/of toestemmingsverklaring voor uw perso-neel. U vindt deze documenten op hoekenblok.nl/avg. In overleg met u kunnen wij deze documenten ook op maat aanleveren.

Privacy nulmeting

Laat een nulmeting uitvoeren, dit geeft u inzicht in de privacy eisen en de nog te nemen stappen.

Privacy-integratie in uw bedrijf

Hoek en Blok heeft een raamwerk ontwikkeld waarin de vereiste privacy-maatregelen zijn vertaald naar algemeen gangbare bestaande bedrijfsprocessen. Hiermee wordt privacy optimaal geïntegreerd in uw bestaande processen Vraag er gerust naar.

Privacy assurance

Wilt u zich onderscheiden in de markt? Laat onze deskundigen uw privacy-processen beoordelen en u hierover rapporteren. Deze rapportage kunt u aan uw klanten overhandigen in commerciële trajecten of op het moment dat uw klant vraagt om naleving van de privacy wetgeving aan te tonen. Zo verstrekt u samen met Hoek en Blok zekerheid over privacy, gebaseerd op de internationale assurance standaard ISAE 3000.

Vragen?

- Kijk op www.AVGwatdoeikermee.nl
- Of stuur een mail naar avg@hoekenblok.nl
- Of bel 0184 496800.

Hoek en Blok Sliedrecht
Stationspark 625
3364 DA Sliedrecht
Postbus 307
3360 AH Sliedrecht
+31 (0)184 49 68 00

Hoek en Blok Barendrecht
Donk 7a
2991 LE Barendrecht
Postbus 35
2990 AA Barendrecht
+31 (0)180 64 54 64

www.AVGwatdoeikermee.nl
avg@hoekenblok.nl

Disclaimer

De AVG is omvangrijk. Deze folder bevat dan ook geen uitputtende lijst van zaken die binnen uw organisatie geregeld dienen te worden. De folder is bedoeld om uw aandacht te vestigen op de AVG en de beginselen daarvan uiteen te zetten. Volledigheid is niet beoogd. Mocht u nog vragen hebben of twijfelen of u zaken op een juiste wijze aanpakt, neemt u dan contact op met Hoek en Blok.

Hoek en Blok
accountants | belastingadviseurs | juristen

Rust en ruimte om te ondernemen