AVG &Boon

Algemene Verordening Gegevensbescherming

INFORMATIE

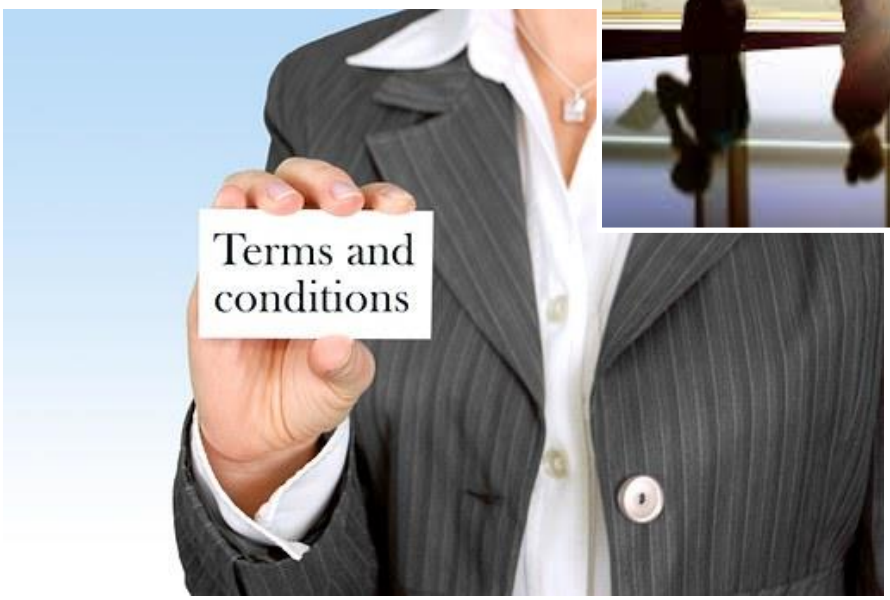
Hoe gaat Boon om
met de privacy wetgeving
AVG/GDPR?

AVG/GDPR
Hoe gaat Boon om met deze privacy wetgeving?

Wat is de AVG/GDPR?

Het vinden van de juiste balans tussen het gebruik van persoonsgegevens en de bescherming van privacy is een van de grootste uitdagingen van het digitale tijdperk. Alle organisaties die binnen de Europese Unie persoonsgegevens verwerken, krijgen onder meer te maken met de Algemene Verordening Gegevens-bescherming (AVG), de nieuwe Europese privacywet. Deze wet is ook wel beter bekend als de General Data Protection Regulation (GDPR).
De AVG vervangt de verouderde Nederlandse Wet bescherming persoonsgegevens (Wbp) en heeft als doel persoonsgegevens beter te beschermen en die bescherming in de gehele Europese Unie gelijk te trekken. Organisaties moeten (nog) duidelijk(er) maken waarom ze persoonsgegevens verzamelen, waarvoor ze die gebruiken en hoe lang de data wordt bewaard.

Per 25 mei 2018 is de AVG van toepassing. Vanaf die datum is alle bestaande regelgeving in de EU gecentraliseerd en aangepast aan het digitale tijdperk. In Nederland is de Autoriteit Persoonsgegevens (AP) het orgaan dat hierop toezicht gaat houden en zal handhaven.



1 Wat verandert er door de komst van de AVG/GDPR?

De AVG versterkt de positie van betrokkenen (de mensen van wie gegevens worden verwerkt). Zij krijgen nieuwe privacyrechten en hun bestaande rechten worden sterker. Organisaties die persoonsgegevens verwerken krijgen meer verplichtingen. De nadruk ligt – meer dan nu- op de verantwoordelijkheid van organisaties om te kunnen aantonen dat zij zicht aan de wet houden.

De komst van de AVG brengt een aantal nieuwe eisen met zich mee:

- organisaties dienen persoonsgegevens nog beter te beschermen;
- indien er sprake is van processen waarbij op grote schaal persoonsgegevens worden verwerkt, dienen deze vastgelegd te worden in een register;
- betrokkene heeft nieuwe rechten zoals het recht om vergeten te worden (‘right to be forgotten’), het recht op inzage, het recht op correctie en het recht op dataportabiliteit;
- Privacy by design & Privacy by default:
  - Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.
  - Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.
- de mogelijkheid voor de toezichthouder (in Nederland de Autoriteit Persoonsgegevens) om hogere boetes op te leggen als een organisatie niet aan zijn wettelijke verplichtingen voldoet.

2 Hoe gaat Boon om met persoonsgegevens?

Boon neemt het beschermen van persoonsgegevens zeer serieus. De AVG hebben wij aangegrepen om ons beleid voor databescherming en dataveiligheid opnieuw in te richten. De nieuwe Europese wetgeving heeft een plaats in onze interne procedures, in de opleiding van medewerkers en in de inrichten van processen, systemen en relevante (interne) documentatie.

De basis van hoe wij met persoonsgegevens omgaan, hebben wij vaststaan in onze gedragscode, die op alle medewerkers van toepassing is:

“We beschermen persoonlijke informatie en andere vertrouwelijke informatie in elke vorm. We verzamelen, bewaren, gebruiken, verzenden en verwijderen persoonlijke en vertrouwelijke informatie op een transparante manier die vertrouwen bevordert. We verzamelen, gebruiken en bewaren persoonlijke informatie, klantinformatie en andere vertrouwelijke informatie alleen als we hiervoor een gegronde reden hebben. Toegang tot deze informatie wordt alleen verleend als dat nodig is. Onze vertrouwelijkheidsplicht eindigt niet als we bij Boon vertrekken; we blijven de vertrouwelijkheid van informatie zelfs na ons vertrek respecteren.”

3 Belangrijke initiatieven

Boon draagt een visie en strategie uit voor de omgang met persoonsgegevens en de bescherming van informatie en hanteert voor elke discipline in haar organisatie een uniform privacybeleid.

Een uniform privacybeleid

Uitgangspunten binnen dit beleid zijn:

Wij beschermen de gegevens die wij ontvangen

- Een medewerker die aan een opdracht werkt, houdt de gegevens die hij of zij ontvangt geheim;
- We gebruiken de gegevens alleen voor het doel waarvoor wij ze ontvangen. Daarom krijgen alleen die collega's die de gegevens nodig hebben om hun taak uit te oefenen, toegang tot deze gegevens (need to know-principe);
- We verwijderen persoonsgegevens direct na het afronden van de opdracht, tenzij de wet of beroepsregels ons verplichten ze te bewaren (bijvoorbeeld voor het aanhouden van een dossier).

Wij beschermen de gegevens die wij versturen of met derden delen

- Als we persoonsgegevens moeten versturen naar landen buiten de Europese Economische Ruimte, handelen we in lijn met toepasselijke wetgeving voor de transfer van persoonsgegevens. We sturen alleen persoonsgegevens als we vereiste, passende waarborgen hebben.
- Als wij externe dienstverleners of andere derden inschakelen die toegang hebben tot persoonsgegevens van onze klanten, dan sluiten we met die partij een (sub-)verwerkersovereenkomst. Wij werken met derde partijen die voldoen aan onze beveiligingsvereisten.

Wij hanteren adequate standaarden

- Wij zorgen ervoor dat persoonsgegevens accuraat, compleet en actueel zijn en blijven;
- Wij treffen passende organisatorische en technische maatregelen om persoonsgegevens adequaat te beveiligen;
- Via de nieuwste technologieën en encryptie worden klant- en persoonsgegevens beveiligd tegen datalekken, ongeautoriseerde toegang of onrechtmatige verwerking.
- Boon heeft een procedure voor het melden van een datalek conform de Wet Meldplicht datalekken.

Privacy Officer

De Privacy Officer (PO) van Boon houdt toezicht op de toepassing en naleving van de AVG. De Privacy Officer is aanspreekpunt voor de interne organisatie, klanten en leveranciers inzake informatiebeveiliging en privacy. De Privacy Officer draagt zorg voor de implementatie van het data privacy programma en waarborgt onze kwaliteitsnormen op het gebied van omgang met persoonsgegevens.

4 Informatiebeveiliging

Boon doet er alles aan om uw (persoons)gegevens te beschermen door middel van fysieke, elektronische en procesgerichte veiligheidsmaatregelen overeenkomstig de actuele stand van de techniek.

Informatiebeveiligingsprogramma
Boon heeft het beheer van haar systemen ondergebracht bij een IT-gespecialiseerde partij die voldoet aan alle eisen zoals gesteld in de ISO27001 standaard. Daarnaast bestaat dit programma onder meer uit de volgende onderdelen:

Disaster & Recovery
Boon werkt voortdurend aan haar disaster & recoveryplan. Dit plan voorziet in de stappen die doorlopen moeten worden om de bedrijf kritische activiteiten en diensten van Boon binnen de vastgestelde tijdsplanning weer operationeel te maken met een zo beperkt mogelijke economische impact.

Individuele verantwoordelijkheid bij het omgaan met (persoons)gegevens.
Gegevens en andere informatie die een medewerker bij zijn of haar werk verkrijgt, mogen alleen worden gebruikt binnen het kader van de opgedragen werkzaamheden.
Voordat deze informatie aan personen binnen of buiten de onderneming wordt doorgegeven, is het de verantwoordelijkheid van elke medewerker om te controleren of de ontvanger het recht heeft om deze informatie te verkrijgen.

Bewustzijn van de medewerkers
Informatiebeveiliging vereist een verhoogd veiligheids-bewustzijn. Onze medewerkers ontvangen op regelmatige basis informatie op het gebied van Data Privacy en Informatiebeveiliging. Daarnaast worden zij continu over de meest recente informatiebeveiligings-kwesties geïnformeerd.

Toegangsbeheersing
We hanteren een consequente functie- en rollenscheiding. Geautoriseerde toegang tot IT-systemen wordt gegarandeerd door 2-weg identificatie van buitenaf op onze interne systemen. Gescheiden rollen bij toegangsverlening zijn verplicht voor IT-systemen die met persoonlijke of vertrouwelijke gegevens werken. Toegang wordt verleend op basis van het 'need to know' en het 'least privileges' principe. Een password management proces specificeert het gebruik en beheer van wachtwoorden. De fysieke toegang tot het pand van Boon wordt gecontroleerd. Servers zijn ondergebracht in fysiek afgesloten serverruimtes dan wel ondergebracht in datacenters met verhoogde toegangscontrole.

Overdracht en bewaren van gegevens
Overdracht van vertrouwelijke of persoonsgegevens vindt enkel plaats door middel van digitale datadragers met versleuteling. Autorisatie voor gegevensoverdracht wordt verleend volgens het 'need to know' principe. Vertrouwelijke gegevens worden niet langer bewaard dan nodig en op een geschikte en veilige wijze vernietigd.

Bescherming tegen ongeoorloofde toegang
Netwerkfirewalls en hackerdetectiesystemen isoleren verschillende netwerkzones, wat een adequaat beveiligingsniveau garandeert.
- Alle netwerkgateways waarmee netwerkverkeer het Boon netwerk binnenkomt of verlaat, worden beschermd;
- De interne structuur van het Boon netwerk is verborgen voor de buitenwereld;
- Laptops zijn uitgerust met 2-way identification op het interne netwerk van Boon van buitenaf, persoonlijke beveiligingssoftware en, waar nodig, versleuteling van de harde schijf. Data wordt alleen in uitzonderingsgevallen op harde schijven van de laptops van onze medewerkers opgeslagen. Alle IT-systemen zijn uitgerust met permanente virusbeveiliging die op virussen controleert en antiviruscontroles uitvoeren bij alle gateways naar het Boon netwerk. Boon kent een control launch of applications waarmee elke applicatie

die gestart wordt geautoriseerd moet zijn voor het interne netwerk.

Audits op het gebied van informatiebeveiliging

Om een vollediger beeld te krijgen van de kwaliteit van onze informatiebeveiliging, worden verschillende vormen van audits uitgevoerd:

- Netwerkzwakte scans (PEN-test), waarbij de focus ligt op de technische aspecten van het informatiebeveiligingsbeleid, zoals patch beheer, applicatiebeveiliging en infrastructuur beveiliging.
- On-site zelfbeoordelingen, waaronder interviews met key management personeel, gedetailleerde werkvloercontroles en documentatiecontrole, die er voor zorgen dat de regels, instructies, voorschriften en wettelijke vereisten worden nageleefd.

5 Wat betekent de komst van AVG voor u?

Uiteraard kunt u dezelfde dienstverlening van Boon verwachten als voorheen. Wij verzekeren u dat we zorgvuldig omgaan met uw persoonsgegevens en verstrekken deze niet aan derden zonder uw toestemming tenzij deze gegevens nodig zijn voor uitvoering van de dienstverlening of wanneer dit wettelijk verplicht is.

Boon dient in haar werkzaamheden aan wettelijke verplichtingen te voldoen en in sommige gevallen onafhankelijk op te treden, hierdoor kent het vormgeven van de privacy rechtelijke positie van Boon een aantal bijzonderheden. Zo kan Boon zowel de rol van verwerker als verwerkingsverantwoordelijke vervullen. Op onze website, www.boon.nl, vindt u onze Privacyvoorwaarden.

In onze Privacyvoorwaarden is uitgewerkt in welke gevallen Boon als verwerkingsverantwoordelijke optreedt en in welke gevallen als verwerker. Onderdeel van de Privacyvoorwaarden is een verwerkers-overeenkomst (bijlage 1) die van toepassing is voor klanten waarbij Boon optreedt als verwerker.

Daarnaast zijn onze Algemene Voorwaarden en ons Privacy Statement geheel in lijn gebracht met de nieuwe privacywetgeving.

Heeft u vragen of opmerkingen, of wilt u een afspraak maken? Neem dan contact met ons op.

Boon Accountants Belastingadviseurs B.V.
Boon Registeraccountants B.V.
Boon Corporate Finance B.V.

Christiaan Geurtsweg 1, 7335 JV Apeldoorn
Telefoon 055-5498500

www.boon.nl