



Impact van de Europese privacy verordening ('AVG') – van Wbp naar AVG, veranderingen in vogelvlucht



15 november 2017

Silvia Vinken CIPP/E

BANNING

LEGAL · TAX

Onderwerpen

- De AVG in het kort
- Van Wbp naar AVG: wat blijft hetzelfde?
- Van Wbp naar AVG: wat gaat er veranderen?
- Voorbereiding op de AVG: tips



BANNING

LEGAL · TAX

Vraag 1

- Wie is er al klaar voor de komst van de Europese privacy verordening per 25 mei 2018?
 - A. Ja, ik ben al compliant
 - B. Nog niet klaar, eerste stappen zijn gezet
 - C. Nee, nog niets gedaan



27-10-2017 | door: **Wouter Hoeffnagel** - redacteur Dutch IT-channel en Executive-People



Bijna twee derde van de Europese bedrijven is niet klaar voor AVG

Het overgrote deel van de Nederlandse bedrijven verwacht dat de Algemene Verordening Gegevensbescherming (AVG) grote impact gaat hebben op de eigen bedrijfsvoering. Toch ligt slechts 36 procent op schema met de voorbereiding op deze nieuwe Europese privacywet.

Dat blijkt uit een peiling van DDMA, de brancheorganisatie voor data en marketing, onder 75 Nederlandse organisaties. De Algemene Verordening Gegevensbescherming (AVG, ook wel bekend onder de Engelse afkorting GDPR) treedt vanaf 25 mei 2018 in werking. Uit de peiling blijkt dat het voor de meeste organisaties een lastige opgave wordt om op tijd klaar te zijn. Slechts 36 procent van de ondervraagden zegt op schema te liggen, iets minder dan de helft maakt plannen om te beginnen en de rest heeft nog helemaal geen voorbereidingen getroffen. Een gebrek aan capaciteit (33%), tijd (25%) en kennis (10%) worden als belangrijkste oorzaken genoemd.

BANNING

LEGAL · TAX

De AVG in het kort

- Algemene Verordening Gegevensbescherming (Vo. 2016/679)
- 25 mei 2018 → vervangt per die datum ook de huidige Wet bescherming persoonsgegevens (Wbp) en de huidige privacyrichtlijn
- Uitvoeringswet (UAVG): nog niet ingediend in Tweede Kamer

Van Wbp naar AVG: wat blijft hetzelfde?

- Thema's blijven hetzelfde maar:
 - er zijn accent- en definitieverschillen;
 - transparantie is nadrukkelijker gedefinieerd;
 - het is EU-wetgeving geworden;

het gedachtegoed van de Wbp (inclusief de meldplicht datalekken) is er nog stevig in terug te vinden.

Tussenconclusie: goed vertrekpunt

Ondernemingen die momenteel op een aantal vlakken al in lijn met de Wbp handelen hebben goed vertrekpunt voor compliance met de AVG



BANNING

LEGAL · TAX

Van Wbp naar AVG: what's new?



- Kort samengevat:
 - Handhaving (boetes)
 - Meer verplichtingen en formaliteiten voor de organisatie, het principe van accountability, anders gezegd: autoverhuurbedrijven moeten altijd uit kunnen leggen wat ze met data doen, waarom ze gegevens verwerken, hoe lang en waarom ze gegevens bewaren, dat ze gegevens goed beveiligen.

Vraag 2

- Wie worden geraakt door de nieuwe privacyregels?
 - A. Klanten
 - B. Werknemers
 - C. Leveranciers
 - D. Alle drie
 - E. Ik weet het niet

What's new?

- De belangrijkste veranderingen op een rij:
 1. Meer verplichtingen voor bewerkers (of: verwerkers)
 2. Meer rechten voor betrokkenen (datasubject)
 3. Veel formaliteiten voor organisaties c.q. de (verwerkings)verantwoordelijke (PIA's, aanstellen FG, verwerkingsregister in kader van documentatieplicht)
 4. Aandacht voor beveiliging van persoonsgegevens
 5. Aangescherpte meldplicht datalekken
 6. Substantiële boetes

Van Wbp naar AVG: what's new?

- Dwingend voorgeschreven invulling van de verwerkersovereenkomst is nieuw ten opzichte van de Wbp en privacyrichtlijn
- Tip: ga tijdig na of u met alle verwerkers wel een overeenkomst hebt gesloten. Denk aan cloud providers, salaris administratie e.d.
- Check of eerdere afspraken mogelijk in andere vorm of andere overeenkomst zijn vastgelegd
- Tip: maak uw bestaande verwerkersovereenkomsten AVG-proof (model overeenkomsten via BOVAG)



Van Wbp naar AVG: what's new?

- Meer rechten voor betrokkenen (= klanten en werknemers):

Nieuw:

1. Uitbreiding informatieplicht (artikel 13 AVG) – privacy statement
2. Recht om vergeten te worden
3. Recht op beperking van de verwerking (artikel 18 AVG)
4. Recht om gegevens mee te nemen (dataportabiliteit)
5. Recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming (o.a. profilering)

Van Wbp naar AVG: what's new?

- Bewaartermijnen: nu al mag een autoverhuurbedrijf gegevens niet langer bewaren dan nodig.
- **Nieuw:** bewaartermijnen zelf moeten worden benoemd in kader van informatieverplichtingen/inzagerechten
- **Nieuw:** Termijn geldt niet alleen om weg te gooien/archiefbestemming te geven, maar ook voor 'periodic review' om gegevens up to date te houden.

Van Wbp naar AVG: what's new?

- Informatieplicht & inzagerecht (bestond al):
 - **Nieuw:** verplichting om meer info te verstrekken (bewaartermijn, mogelijkheid klacht in te dienen, veiligheidsmaatregelen)
 - **Nieuw:** geen kosten behalve in geval van bijkomende kopieën

Vraag 3

- U wordt benaderd door politie/justitie die informatie wil hebben over een persoon die een auto gehuurd heeft. Verstrek u deze?
 - A. Ik verstrek deze altijd. Aan politieverzoeken moet je altijd gehoor geven
 - B. Hangt er van af. Ik vraag de politie om de grondslag van het verzoek nader toe te lichten
 - C. Ik weiger de informatie te verstrekken om de privacy van de huurder te allen tijde te respecteren

Vraag 4

- Als een klant een beroep doet op het 'right to be forgotten' dan moet het autoverhuurbedrijf alle data verwijderen die zijn vastgelegd

A. Ja

B. Nee

Van Wbp naar AVG: what's new?

- Veel formaliteiten voor organisaties:
 - PIA's (Privacy impact assessment) – *niet altijd verplicht*
 - Documentatieplicht voor grote autoverhuurbedrijven (accountability) – *van trust me naar show me*
 - Comply or explain
 - Verwerkingenregister
 - (Formele) FG / DPO aanstellen – *nvt voor autoverhuurbedrijven*

Van Wbp naar AVG: what's new?

- Veel formaliteiten voor organisaties:
 - PIA's (Privacy impact assessment) – artikel 35 AVG
 - Vereist indien:
 - *Profilering met rechtsgevolgen voor natuurlijke personen of die natuurlijke personen wezenlijk treft;*
 - *Grootschalige verwerking van bijzondere persoonsgegevens*
 - *Stelselmatige grootschalige monitoring van openbaar toegankelijke ruimten*
- Beoordelingsvrijheid verwerkingsverantwoordelijke
- Autoriteit Persoonsgegevens ('AP') kan zwarte en witte lijsten opstellen

Vraag 5

- Moet er een PIA worden gedaan als het autoverhuurbedrijf besluit om elke auto te voorzien van een track & trace systeem?

A. Ja
B. Nee

Van Wbp naar AVG: what's new?

- **Nieuw:** privacy by design: verplichting om bij ontwikkelen van producten/processen rekening te houden met gegevensbescherming
- **Nieuw:** privacy by default: verplichtingen om de instellingen en functies van producten of diensten, standaard (by default) op de hoogst mogelijke privacy stand hebben staan

Van Wbp naar AVG: what's new?

- Veel aandacht voor beveiliging
 - Wbp bepaalt dat je moet beveiligen, de AVG zegt hoe
 - Bescherming persoonsgegevens kan niet los worden gezien van een deugdelijk beveiligingsbeleid
 - Beveiliging ziet ook op organisatorische aspecten (denk aan sleutelbeleid, clean desk, geheimhoudingsverklaringen personeel e.d.)
 - Centrale rol voor IT / Security

Van Wbp naar AVG: what's new?

- Aangescherpte meldplicht datalekken
 - Bestond al onder de Wbp, geen grote wijzigingen onder de AVG
 - AVG stelt strengere eisen aan de registratie van datalekken: alle datalekken moeten worden geregistreerd (gaat verder dan de huidige Wbp die enkel verplicht tot registreren gemelde datalekken)
 - Tip: zorg voor een datalekkenprotocol



DATABESCHERMING

Richtlijn datalekken kan bedrijven miljoenenboetes opleveren

Rutger Betlem
Amsterdam

Het bedrijfsleven voelt nu al de impact van de grote wetswijziging rond databescherming die volgend jaar van kracht wordt. Experts waarschuwen voor de gevolgen van de invoering van de nieuwe algemene verordening gegevensbescherming (AVG), de grootste wetswijziging op dit gebied in twee decennia.

De eisen uit de Europese privacywetgeving zijn strenger dan de huidige Wet bescherming persoonsgegevens (WBP). Wie verkeerd omgaat met persoonsgegevens kan vanaf 25 mei 2018 een boete opgelegd krijgen tot 4% van de jaaronzet, of € 20 mln.

'Datalekken waarbij persoonsgegevens zijn verloren of gestolen, moeten sneller gemeld worden en we kunnen eerder boetes uitdelen', zegt Aleid Wolfsen, voorzitter van de

Autoriteit Persoonsgegevens. 'In de WBP moest er sprake zijn van opzet of grove schuld, deze bepaling verdwijnt. Beveiliging moet topprioriteit zijn.'

'Bedrijven en overheden moeten er straks met de AVG voor zorgen dat ze meer grip en controle krijgen op wat er met hun data gebeurt', zegt Diana Janssen, voorzitter van DDMA, de brancheorganisatie voor databasemarketing.

De wet geldt niet alleen voor Europese bedrijven en instituten. Ook internationale partijen, zelfs als ze geen vestiging in Europa hebben, moeten zich aan de regels houden als ze gegevens verwerken van Europeanen.

Volgens Janssen stellen vooral de nieuwe documentatieplicht en de verplichte privacy-administratie bedrijven voor uitdagingen. Van alle data moet minutieus in kaart

gebracht worden waar ze vandaan komen, hoe ze beveiligd zijn en wie er toegang toe heeft. Bedrijven die hun klanten benaderen, moeten voorafgaand aan iedere actie voortaan een analyse uitvoeren van de impact op privacy.

Het belangrijkste doel van de wetswijziging is de burger meer macht geven. Ondernemingen en overheden moeten duidelijk maken waarom ze bepaalde gegevens willen vragen en waarvoor ze die gebruiken. Daarnaast krijgen burgers meer zeggenschap over hun data. Zo geldt het recht om vergeten te worden, maakt dataportabiliteit bij het overstappen naar een andere leverancier deel uit van de bepaling en kunnen burgers laagdrempelig een klacht indienen bij de toezichthouder en inzage vragen in de data die over ze opgeslagen is. Toestemming in trekken moet net

zo makkelijk worden als toestemming geven.

Een instantie of bedrijf moet verder een functionaris gegevensbescherming (FG) aanstellen. Janssen: 'Dat er zoveel FG's nodig zijn, is al een issue op zich, zeker voor grote bedrijven. Als je nog niet zo'n functionaris op het oog hebt, dan zou ik daar snel mee beginnen. Tegen mei 2018 zal de spoeling dun zijn.' De FG krijgt een bijzondere rechtsspositie binnen het bedrijf. De functionaris opereert onafhankelijk en kan minder makkelijk ontslagen worden.

'Je zult in ieder geval iemand in het bedrijf verantwoordelijk moeten stellen voor de meldplicht', vertelt Bastiaan Bakker van cybersecuritybedrijf Motiv. 'Het kan niet zo zijn dat iemand van de IT-afdeling lukraak meldingen gaat doen.'

Volgens de ondernemer ontstaan de meeste problemen door



Overal waar personeel met gevoelige informatie werkt, lopen bedrijven risico's. FOTO: HH

dat per ongeluk data gelekt worden, denken aan het automatisch aanvullen van e-mailadressen waardoor een mailtje naar de verkeerde persoon gestuurd wordt. Om de deadline van 2018 te kunnen halen, raadt Bakker ondernemers aan in ieder geval te kijken naar de bewerksovereenkomsten van leveranciers, oude en overtollige data te verwijderen en om data zo veel mogelijk te consolideren op één plek. 'Dat de IT is uitbesteed, betekent niet dat je niets hoeft te doen.'

Janssen vindt dat bedrijven serieuzer om moeten gaan met de gegevens van hun klanten. 'Er wordt binnen de boardrooms te weinig nagedacht over wat een bedrijf wil met data. Het wordt te vaak overgelaten aan de marketing- en salesafdeling. Waarom maakt privacy niet naast duurzaamheid een vast deel uit van het jaarverslag?'

BANNING

LEGAL · TAX

Vraag 6

- Een gebruiker van een deelauto vergeet uit te loggen. De volgende gebruiker ziet de navigatiegegevens van de eerste gebruiker. Is dit een datalek?
 - A. Ja
 - B. Nee
 - C. Ik weet het niet

Van Wbp naar AVG: what's new?

- Substantiële boetes, twee categorieën:
 - Minder zwaar: max EUR 10 mio tot 2% van de totale wereldwijde omzet (o.a. niet voldoen aan de plicht om een register bij te houden)
 - Zwaar: max EUR 20 mio tot 4% van de totale wereldwijde omzet (o.a. niet naleven basisbeginselen van gegevensverwerking, rechten van betrokkene waarborgen etc.)



BANNING

LEGAL · TAX

Van Wbp naar AVG: what's new?

- Substantiële boetes
 - Handhaving door AP (ook persoonlijke boetes mogelijk voor directie en/of medewerkers)
 - Bestuurlijke toezichthouder, vergelijkbare bevoegdheden als bijvoorbeeld ACM
 - Tip: wees voorbereid op een bezoek van de AP, zorg voor een invalprotocol



Conclusie

- Van Wbp naar AVG: veel is hetzelfde gebleven
- Maar ook nieuwe elementen: accountability, meer rechten voor betrokkenen, meer verplichtingen voor organisaties
- Aantal zaken nog onduidelijk: moet praktijk uitwijzen
- Niet vrijblijvend: op straffe van sancties

Vorbereiding op de AVG: tips

NIEUWS

NALEVING NIEUWE PRIVACYREGELS: NUCHTER DENKEN VOLDOET

📅 9 maart 2017 ⌚ 3 min. leestijd



redactie Mr.

in LinkedIn

f Facebook

🐦 Twitter

✉ Email

De nieuwe **Europese verordening op de privacy** leidt echt niet tot allerlei cowboy-toestanden. Ja, de rechten van de burger worden aanmerkelijk versterkt, maar ook voor de privacyregelgeving geldt dat iedereen die een beetje logisch nadenkt best weet wat wel of niet kan.

Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens, probeerde dinsdagmiddag, aan het eind van een congres in congrescentrum Papendal bij Arnhem, door dit statement de zaal een beetje gerust te stellen. Hij kreeg de lachers op z'n hand toen hij een vergelijking trok met de studie rechten: "Was het niet zo dat toen bij een tentamen, als we weer eens niet geleerd hadden, toch een voldoende kregen als we gewoon opschreven wat ins ons opkwam na een beetje rustig nadenken? Zo is het ook bij privacywetgeving. Het gaat met name over de bestrijding van de uitwassen. Organisaties en bedrijven die zich fatsoenlijk gedragen hebben echt niets te vrezen."



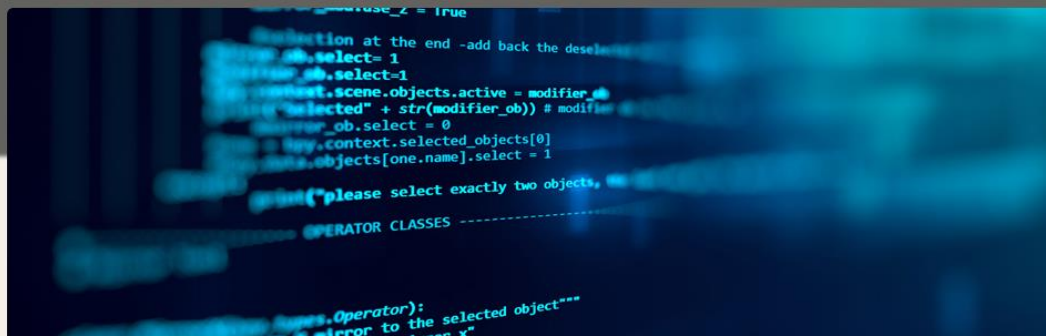
Legal Valley-voorzitter Fred Hammerstein (l) en Aleid Wolfsen (Autoriteit Persoonsgegevens). Foto Chris van Houts

Vorbereiding op de AVG: tips

- Betrek de directie tijdig bij het maken van een privacy beleid
- Plan organisatorische en budgettaire maatregelen in
- Formeer een team en maak een projectplan
- Begin bij het begin: inventariseer de belangrijkste gegevensstromen en bedrijfsprocessen. Maak een analyse van de belangrijkste privacy risico's
- Maak bestaande documenten AVG-proof (review bewerkersovereenkomsten, datalekkenprotocol, privacy statement + cookie disclaimer)

Vorbereiding op de AVG: tips

Wacht met aanschaf: BOVAG komt in december met privacytool



Er gaat een nieuwe strenge privacywet in op 25 mei 2018. U moet persoonsgegevens nog meer beschermen en de overheid gaat strikter handhaven. Naar verwachting kunt u vanaf december gebruik gaan maken van de BOVAG-tool, die u helpt te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Er zijn commerciële hulpmiddelen op de markt, maar het loont om nog even te wachten met de aankoop ervan. De tool van BOVAG is namelijk helemaal op maat gemaakt voor de mobiliteitsbranche.

BANNING

LEGAL · TAX

Vorbereiding op de AVG: tips

- Respecteer rechten van betrokkenen -> maak onderscheid intern (werknemers) en extern (klanten). Procedures voor inzage en correctie en bewaartermijnen (vergeet de OR niet)
- Uitrol van een beveiligingsbeleid (hoofdrol voor IT en Security). Aansluiten bij bestaande normen als ISO27001?
- Besteed blijvend aandacht aan awareness (trainen en voorlichten medewerkers)

“The best way to **protect data security** is to get rid of all the **human**.”

Plan B is to **train** them.”

BANNING

LEGAL · TAX

Vragen?

- Contactgegevens:
 - Silvia Vinken (s.vinken@banning.nl) / 06 51508536 / 073 69 27 715

BANNING

LEGAL · TAX