CHECKLIST PRIVACY AVG

Privacybeleid in 46 checklists

Van WBP naar AVG en UAVG

CHECKLIST PRIVACY AVG

Privacybeleid in 46 checklists

Van WBP naar AVG en UAVG

Tweede druk

Auteurs:
Prof. mr. J.M.A. Berkvens
Mr. S.M.M.C. Vinken CIPP/E
Mr. S.R. Wiegerinck
Mr. S.W.G. Wolters
J. Reijner
Mr. M.J.M.G. van Gerwen

Berghauser Pont Publishing

Berghauser Pont Publishing
Postbus 14580
1001 LB Amsterdam
www.berghauserpont.nl
Omslagontwerp: Rosanna Zito, Zedline.
2e druk, 2018
ISBN: 9789492952011
NUR: 823

© 2018 Berghauser Pont Publishing

Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van art. 16h Auteurswet 1912 dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan Stichting Reprorecht (Postbus 3060, 2130 KB Hoofddorp, www.reprorecht.nl). Voor het overnemen van gedeelte(n) uit deze uitgave in bloemlezingen, readers en andere compilatiewerken (art. 16 Auteurswet 1912) kan men zich wenden tot Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, Postbus 3060, 2130 KB Hoofddorp, www.cedar.nl/pro).

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg besteed is, aanvaarden de auteur(s), redacteur(en) en uitgever geen enkele aansprakelijkheid voor eventuele (druk) fouten en onvolledigheden, noch voor gevolgen hiervan.

All rights reserved. No part of this publication may be reproduced in any form, by print, photo print, microfilm or any other means, without the publishers prior written permission.

Voorwoord

Bij de tweede druk

Sinds het verschijnen van de eerste druk van dit boek in 2016 is de betekenis van de Algemene verordening gegevensbescherming (AVG) voor de praktijk steeds duidelijker geworden. Op 12 december 2017 is een implementatiewet AVG in de Tweede Kamer ingediend (UAVG). Deze is op 13 maart 2018 aangenomen door de Tweede Kamer en naar de Eerste Kamer gezonden. De Europese privacy toezichthouders hebben door middel van een groot aantal nieuwe of gereviseerde opinies de bepalingen uit de AVG van hun uitleg voorzien. Vanaf 25 mei 2018 is de Wbp vervallen. Bestaande verplichtingen zijn gewijzigd en nieuwe verplichtingen zijn geïntroduceerd.

In de tweede druk zijn deze ontwikkelingen verwerkt. De eerste druk droeg nog de signatuur van overgang van Wbp naar AVG. De tweede druk is volledig op de AVG gebaseerd. De eerste druk bevatte 32 checklists. Het aantal checklists is in de tweede druk fors uitgebreid. De inhoud van de checklists is bijgewerkt. Nieuwe thema's (DPIA, privacy by design, data portabiliteit, profilering, leidende toezichthouder, registerplicht etc.) komen uitgebreid aan bod. Nieuw is ook de toevoeging van een boetetabel. Die kan in het nieuwe regime niet ontbreken. De checklists bevatten gerichte verwijzingen naar zowel de AVG (inclusief de overwegingen), de relevante bepalingen in de UAVG als de adviezen van Europese privacy toezichthouders. De tweede druk bevat gemakshalve nog steeds de wettekst van de Wbp. Ook is de tekst van de op 13 maart 2018 bij de Eerste Kamer ingediende implementatiewet opgenomen. Hoofdstuk 8 van de Memorie van Toelichting bij de implementatiewet is eveneens opgenomen. Dit bevat een overzichtelijke implementatietabel (transponering AVG naar UAVG naar WBP). De transponeringstabel AVG-Wbp uit de eerste druk is daarmee komen te vervallen. Bij de tweede druk is in aanvulling op de tabel Wbp -> AVG een nieuwe transponeringstabel opgenomen (UAVG -> AVG) evenals een checklist die betrekking heeft op de overgangssituatie van Wbp naar AVG.

Wij spreken de hoop uit dat dit boekwerk een nuttige bijdrage levert aan uw implementatiewerkzaamheden.

De bronnen zijn geraadpleegd tot maart 2018.

's-Hertogenbosch, maart 2018

Bij de eerste druk
Het opzetten van een praktische en deugdelijke privacy policy

Zorg voor privacy is geen vrijblijvende aangelegenheid. Dagelijks verschijnen in de media berichten over nieuwe wettelijke regels, datalekken, hacks, onderzoeken van toezichthouders en hoge boetes. Berichten die relevant zijn voor werkgevers en medewerkers, overheidsinstellingen en burgers alsmede voor bedrijven en consumenten. Bij het gebruiken van computers en smartphones wordt men steeds vaker geconfronteerd met verwijzingen naar privacy policies. Frequent wordt gevraagd om toestemming voor het gebruik van persoonsgegevens. De hoeveelheid wettelijke regels op het gebied van privacybescherming neemt toe. De Algemene Verordening Gegevensbescherming ('AVG') [Verordening (EU) 2016/679] van 24 mei 2016, die op 25 mei 2018 in werking gaat treden, zal gevolgen hebben voor alle organisaties en hun gegevensverwerkende processen. Met name omdat er meer eisen gesteld worden op het gebied van het informeren van klanten en medewerkers, het beveiligen van gegevens en het in control zijn. Organisaties doen er daarom verstandig aan zich tijdig te bezinnen op de betekenis van deze verordening.

Wij zien in de praktijk veel organisaties binnen de overheid en het bedrijfsleven worstelen met de vraag of zij nog voldoen aan de vele eisen die de privacywetgeving aan hen stelt, welke risico's zij lopen als zij niet (meer) compliant zijn en wat zij moeten doen om alsnog compliant te worden.

Het compliant maken van een organisatie vereist een serieuze inspanning. Startpunt daarbij is het in kaart brengen van de bedrijfsprocessen,

zodat duidelijk wordt waar de risico's zitten. Vervolgens moeten er maatregelen worden getroffen om deze risico's blijvend te minimaliseren. Er moeten procedures komen voor inzage en correctie. Bewaartermijnen moeten worden vastgesteld. Er moeten procedures komen voor de afwikkeling van datalekken. Websites en communicatieprocessen moeten worden aangepast. Medewerkers zullen daarbij worden ondersteund via zogeheten bewustwordingsprogramma's. Ook zal soms de discussie met het publiek moeten worden aangegaan. Het compliant maken van een organisatie is dus uitdagend. Het is bovendien geen vrijblijvende aangelegenheid. Niet compliant zijn kan voor de organisatie tot negatieve gevolgen leiden. Maar, waar moet je beginnen, en hoe houd je overzicht?

Het vaststellen van een privacybeleid en het vastleggen daarvan in een privacy policy kan helpen bij het in kaart brengen van de belangrijkste aandachtspunten en vormt een goede stap in de richting van een deugdelijk compliance programma op het gebied van privacy. Een privacy policy kan algemeen zijn van aard of specifiek inzoomen op bepaalde domeinen zoals personeel of klanten.

Dit boekje helpt bij het opzetten van zo'n praktische en deugdelijke privacy policy. Onze insteek daarbij is geweest om de checklists voor een brede doelgroep toegankelijk te maken, van juristen en compliance officers tot managers, ICT'ers en auditors, zonder daarbij te veel te verwijzen naar relevante wetsartikelen. Uiteraard bevat de bundel wel de teksten van de Wbp en de AVG (inclusief twee handige transponeringstabellen) zodat u als lezer alle relevante informatie binnen handbereik heeft (zie ook hierna onder 'naslag'). Dit boekje bestaat uit checklists op hoofdlijnen. Ter toelichting daarop het volgende. In hoofdstuk 3 wordt een schets gegeven van de voorbereiding op het schrijven van een privacy policy. Het is belangrijk dat deze voorbereidingen op een voldoende hoog niveau binnen de organisatie worden gedragen. In hoofdstuk 4 wordt aangegeven waarom de 'tone at the top' essentieel is voor het succesvol implementeren van uw privacy policy. In hoofdstuk 5 wordt een aantal algemene aandachtspunten bij het opstellen van een privacy policy genoemd.

Het opstellen van een privacy policy begint vervolgens met het vaststellen wie er verantwoordelijk zijn voor de verwerking van persoonsgegevens (hoofdstuk 6) en voor welk doel persoonsgegevens worden verwerkt (hoofdstuk 7). Hoofdstuk 8 gaat in op de vraag welke informatie beschikbaar moet zijn om in control te kunnen zijn en verantwoording te kunnen afleggen (accountability). Hoofdstuk 19 gaat in op het vaststellen van bewaartermijnen. Afhankelijk van de omvang van uw organisatie kan het raadzaam zijn een privacy-coördinator of een formele Functionaris voor de gegevensverwerking ("FG") aan te stellen. Dat kan een parttime activiteit zijn die gecombineerd kan worden met een al bestaande functie. Voor sommige organisaties zal een FG verplicht worden. Aandachtspunten voor de FG (of een eventuele coördinator) zijn opgenomen in hoofdstuk 9. Centraal onderdeel van de implementatie is de inrichting van een beveiligingsorganisatie en het signaleren en afhandelen van inbreuken. Hoofdstukken 10 (beveiliging), 11 (datalekken), 20 (auditplan) en 21 (onderzoek door toezichthouder) geven daarbij guidance.

De verantwoordelijkheid van organisaties strekt zich ook uit tot de (al dan niet in de cloud) uitbestede verwerking van persoonsgegevens. De wet stelt eisen aan een dergelijke uitbesteding. Hoofdstuk 12 geeft een overzicht van daarbij relevante aandachtspunten. Hoofdstuk 13 is van belang bij grensoverschrijdend persoonsgegevensverkeer buiten Europa.

Het boekje bevat daarnaast diverse andere checklists die behulpzaam zijn bij het uitwerken van onderdelen van de privacy policy:

- voor wat betreft de rechten van een betrokkene verwijzen we naar de checklists voor het vragen van toestemming (hoofdstuk 14) en checklists voor het inrichten van procedures voor informatieverstrekking (hoofdstuk 16), inzage (hoofdstuk 17) en correctie (hoofdstuk 18);
- hoofdstuk 15 besteedt aandacht aan afwijkende regels ten aanzien van minderjarigen;
- in de hoofdstukken 22 t/m 28 worden thema's met betrekking tot personeel uitgewerkt;
- de hoofdstukken 29 t/m 32 gaan in op e-Commerce gerelateerde onderwerpen.

Naslag. Tot 25 mei 2018 hebben we nog te maken met de Wbp. Vanaf die datum gaat nieuwe, op de AVG gebaseerde, wetgeving gelden. Om gemakkelijk tussen de Wbp en de AVG te kunnen schakelen is een naslag met de teksten van beide regelingen in dit boekje opgenomen. Tevens zijn transponeringstabellen opgenomen waarmee vanuit de Wbp de corresponderende bepaling in de AVG kan worden opgezocht en vice versa. Daarbij dient men zich te realiseren dat de AVG sommige onderwerpen (bij voorbeeld de verwerking van strafrechtelijke gegevens) ter verdere uitwerking aan de nationale wetgever overlaat. Van dergelijke uitwerkingen zijn nog geen concrete voorstellen gepubliceerd. Ook kan de wetgever op sommige onderwerpen in algemene of sectorspecifieke regels nog afwijken van de AVG.

Het boekje sluit af met een lijst van gebruikte afkortingen en een overzicht van documentatie waarnaar in het boekje wordt verwezen.

Wij wensen u succes bij de voorbereiding van uw organisatie op de komende invoering van de AVG.

Inhoud