Checklist Privacy AVG

Privacybeleid in 57 checklists

Derde druk

Auteurs:

Prof. mr. J.M.A. Berkvens
Mr. F.H.M. Eijdems
Mr. M.J.M.G. van Gerwen
Mr. K. Knook
Mr. W. Weijland
Mr. S.R. Wiegerinck
Mr. S.W.G. Wolters

Bevat geactualiseerde bijdragen van:

Mr. M.P.M. Hennekens CIPP/E
J. Reijner
Mr. S.M.M.C. Vinken CIPP/E

Berghauser Pont
PUBLISHING

Berghauser Pont Publishing
Postbus 14580
1001 LB Amsterdam
www.berghauserpont.nl

Omslagontwerp: Rosanna Zito, Zedline.
3e druk, 2019
ISBN: 9789492952202

NUR: 823

Voorwoord

Bij de derde druk
Sinds de verschijning van de tweede druk van dit boek in maart 2018 zijn de nodige officiële publicaties verschenen, die van belang zijn voor de toepassing en de uitleg van de AVG. De Europese Artikel 29-werkgroep en haar opvolger, de European Data Protection Board, hebben een tiental nieuwe richtlijnen gepubliceerd. De Autoriteit Persoonsgegevens (AP) heeft nieuwe boetebeleidsregels gepubliceerd. Daarnaast hebben de AP en overheidsinstanties zich intensiever gericht op voorlichting over de (uitleg van de) AVG, via diverse voorlichtingssites en op de website van de AP zelf. Het Europese Hof van Justitie heeft enkele belangrijke uitspraken gedaan over kernbegrippen uit de AVG. Tot slot heeft de tekst van de UAVG op diverse technische punten wijziging ondergaan en zijn nieuwe regels over het toezicht op betaaldienstverleners in de UAVG verwerkt.

Deze derde druk bevat een actualisatie van de bestaande checklists. Daarnaast is een aantal nieuwe checklists toegevoegd, waardoor het aantal is uitgebreid van 46 naar 57. De checklists zijn gehergroepeerd. De hoofdstructuur van het boek is echter ongewijzigd gebleven. De naslag bevat de actuele tekst van de AVG (inclusief het corrigendum uit *PbEU 2018, L 127/2* van 23.5.2018) en van de UAVG. De Wbp blijft eveneens gemakshalve beschikbaar in de naslag.

Wij spreken de hoop uit dat dit boek een nuttige bijdrage kan leveren aan het "AVG-proof" houden van uw bedrijfsvoering.

De bronnen zijn geraadpleegd tot juli 2019.

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.

Inhoudsopgave

Voorwoord		**V**
1	**Wetgeving als drijfveer voor privacybeleid**	**1**
2	**Hoofdlijnen van een privacybeleid**	**3**
3	**Privacy awareness**	**5**
4	**Voorbereiden organisatie**	**7**
5	**Waarom moet de directie worden betrokken**	**9**
6	**Opstellen van een privacybeleid**	**11**
7	**De verwerkingsverantwoordelijke en andere actores**	**13**
8	**De doelomschrijving en de verwerkingsgrondslagen**	**17**
9	**Documentatie, accountability en assurancesystemen**	**21**
10	**Register van verwerkingen (art. 30 AVG)**	**27**
11	**De Functionaris voor de gegevensbescherming FG/DPO**	**31**
12	**Inrichting beveiliging**	**33**
13	**Bewaartermijnen**	**39**

14	**Privacy by design and default**	**43**
15	**Data protection impact assessment (DPIA)**	**47**
16	**Procedure meldplicht datalekken**	**51**
17	**Verwerkersovereenkomsten**	**55**
18	**Cloud computing**	**61**
19	**Aandachtspunten bij internationaal gegevensverkeer**	**63**
20	**Binding Corporate Rules**	**65**
21	**Leidende toezichthouder**	**67**
22	**Eisen aan toestemming als verwerkingsgrondslag**	**71**
23	**Aandachtspunten bij het verwerken van persoonsgegevens van kinderen**	**73**
24	**Eisen aan de informatieplicht**	**75**
25	**Procedure voor inzage persoonsgegevens**	**79**
26	**Wob en bescherming persoonsgegevens**	**83**
27	**Overdraagbaarheid van gegevens (dataportabiliteit)**	**87**
28	**Procedure voor correctie en verwijdering persoons gegevens (right to be forgotten)**	**89**

29	**Profilering**	**93**
30	**Rechtsbescherming (art. 79 AVG en art. 34 en 35 UAVG)**	**97**
31	**Medezeggenschap**	**101**
32	**Personeelsdossiers**	**103**
33	**Identificatie bij indiensttreding**	**105**
34	**Screening van sollicitanten en medewerkers**	**107**
35	**Gegevens van zieke medewerkers**	**109**
36	**Fraudeonderzoek op de werkvloer**	**111**
37	**Gebruik beeldmateriaal van medewerkers**	**113**
38	**Cameratoezicht op de werkvloer (voor controle-doeleinden)**	**115**
39	**Opnemen van gesprekken tussen werkgever en medewerker**	**117**
40	**Alcohol- en drugstesten op de werkvloer**	**119**
41	**Privégebruik van social media: beleid en controle**	**121**
42	**Klokkenluidersregeling**	**123**
43	**De rol van de zzp'er**	**125**

44 Apps 127

45 Wifitracking 129

46 Professionele wearables binnen de organisatie 131

47 E-Commerce / online marketing 133

48 Cookies 137

49 Aanvraag Voorafgaande Raadpleging 141

50 Zwarte lijst (of branchewaarschuwingssysteem) 143

51 Verwerking van persoonsgegevens voor journalistieke doeleinden 145

52 Aansprakelijkheid onder de AVG 147

53 Schadevergoeding ten gevolge van aansprakelijkheid (art. 82 AVG) 149

54 Aandachtspunten bij onderzoek door een toezichthouder 151

55 Klachtprocedure bij de Autoriteit Persoonsgegevens 155

56 Checklist overgangsrecht AVG 157

57 Aandachtspunten voor de auditor 159

Bijlagen 161

Bijlage 1: Transponeringstabel van Wbp naar AVG 163

Bijlage 2: Transponeringstabel van UAVG naar AVG 165
Bijlage 3: Transponeringstabel van AVG naar UAVG en Wbp 166
Bijlage 4: Boetetabel AVG 177

Gebruikte afkortingen 185

Relevante links 187

Naslag 191

Tekst AVG 191
Tekst UAVG 289
Tekst Wet Bescherming persoonsgegevens 305

Achtergrondinformatie 329

Trefwoordenregister 333

1 Wetgeving als drijfveer voor privacybeleid

Het privacybeleid kan worden herleid tot een aantal wereldwijd geaccepteerde privacybeginselen. Die vormen de basis voor nationale en internationale regels. Deze regels zijn te vinden in algemene wetgeving en als onderdeel van specifieke wetten. Hieronder een kleine selectie:

- ☐ OECD Privacy Framework 2013 (revised, zie ook checklist 2);
- ☐ Verdrag 108 Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens;
- ☐ Handvest van de grondrechten van de Europese Unie (art. 7 en 8);
- ☐ Grondwet (art. 10);
- ☐ Europees verdrag voor de rechten van de mens (EVRM) (art. 8);
- ☐ Internationaal verdrag inzake burgerlijke en politieke rechten (IVBPR), art. 17;
- ☐ Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (tot 25 mei 2018);
- ☐ Interpretaties van Richtlijn 95/46/EG als verwoord door de zogenoemde Artikel 29-werkgroep (Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens – WP 29) en gepubliceerd op hun website https://ec.europa.eu/newsroom/article29/news-overview.cfm;
- ☐ Interpretaties van Verordening (EU) 2016/679 (AVG) door de opvolger van WP 29, het Europees Comité voor de Gegevensbescherming (ECG) of European Data Protection Board (EDPB) en gepubliceerd op hun website https://edpb.europa.eu/;
- ☐ Wet bescherming persoonsgegevens (tot 25 mei 2018) (*Stb.* 2000, 302);
- ☐ Richtlijn 2002/58/EG gewijzigd door 2009/136/EG (ePrivacy richtlijn);
- ☐ Telecommunicatiewet (Wet van 19 oktober 1988, houdende regels inzake de telecommunicatie);
- ☐ Wet op de Ondernemingsraden (WOR);
- ☐ Wetten met impact op gegevensverwerking (zoals de Wet op de Geneeskundige behandelingsovereenkomst, art. 7:446-468 BW);
- ☐ Verordening (EU) 2016/679 (AVG) betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (vanaf 25 mei 2018);
- ☐ Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) (*Stb.* 2018, 144);
- ☐ Aanpassingswet Algemene verordening gegevensbescherming (*Stb.* 2018, 247) en Aanpassingsbesluit Algemene verordening gegevensbescherming (*Stb.* 2018, 249 en *Stb.* 2018, 250).

De AVG is per 25 mei 2018 in werking getreden en werkt rechtstreeks door in Nederland. De AVG is door middel van een implementatiewet ingevoerd, Uitvoeringswet AVG (UAVG). Dat is nodig omdat de AVG de regeling en uitvoering van sommige onderwerpen overlaat aan de nationale wetgever. Denk bijvoorbeeld aan bepalingen zoals art. 9 AVG en art. 23 UAVG over de verwerking van bijzondere categorieën van persoonsgegevens.

2 Hoofdlijnen van een privacybeleid

Een privacybeleid is gericht op betrokkenen. Voor bedrijven zijn betrokkenen bijvoorbeeld medewerkers, klanten en/of patiënten. Voor overheden zijn dit ambtenaren en burgers. Een privacybeleid kan ook het karakter hebben van een instructie aan de medewerkers of ambtenaren of onderdeel uitmaken van een bedrijfsreglement of zijn neergelegd in een privacyhandboek. De wijze waarop dit gebeurt is aan de keuze van de betreffende organisatie. Bij het opstellen van een privacybeleid (zie ook art. 24 lid 2 AVG) kunnen de volgende hoofdlijnen (uitgangspunten uit de wetgeving) worden gevolgd:

Algemene privacybeginselen:
(Zie ook hierna OECD Privacy Framework 2013, Part Two. Basic Principles of National Application)
- ☐ aanwijzing van een voor de verwerking verantwoordelijke rechtspersoon;
- ☐ omschrijving van verwerkingsdoelen van persoonsgegevens;
- ☐ vaststellen welke persoonsgegevens redelijkerwijs nodig zijn voor het doel (proportionaliteit en subsidiariteit);
- ☐ check op wettelijke grondslagen (art. 6 AVG);
- ☐ opstellen van kwaliteitseisen die worden gesteld aan persoonsgegevens;
- ☐ vaststellen van bewaartermijnen;
- ☐ procedures bij hergebruik van gegevens (doelconform en "niet onverenigbaar met verzameldoel");
- ☐ informeren van betrokkenen;
- ☐ rechten van betrokkenen (zoals inzage en correctie);
- ☐ inrichting van beveiliging.

Bijzondere onderwerpen:
- ☐ uitbesteding;
- ☐ meldplichten bij datalekken;
- ☐ doorgifte persoonsgegevens naar buitenland;
- ☐ geschillenprocedure;
- ☐ controlemechanismen (audit).

Organisatiespecifieke thema's:
- ☐ gegevens die bijzondere aandacht vereisen;
- ☐ personen die bijzondere aandacht vereisen;
- ☐ verwerking persoonsgegevens via social media;
- ☐ voice logging;
- ☐ camera's;
- ☐ fraudebestrijding;
- ☐ gebruik biometrische gegevens;
- ☐ gebruik medische gegevens.

De AVG maakt het noodzakelijk om een goede beschrijving van het privacybeleid beschikbaar te hebben. Dat kan door het beleid in een privacypolicy vast te leggen (art. 5 lid 2 AVG en art. 24 lid 2 AVG).

Een privacybeleid of -policy is overigens iets anders dan een privacyverklaring. Alle organisaties die persoonsgegevens verwerken moeten betrokkenen heldere informatie verstrekken over onder andere de persoonsgegevens die zij verwerken en voor welk(e) doel(en) zij deze gegevens verwerken (zie ook checklist 24). De meest aangewezen manier hiervoor is het opstellen van een (online) privacyverklaring.

3 Privacy awareness

E-mailblunders, zwakke wachtwoorden, het openen van besmette e-mailbijlagen, kwaadwillend personeel en het niet installeren van beveiligingsupdates zijn voorbeelden van fouten die (onbewust) door mensen gemaakt worden met mogelijk grote gevolgen. Alle genomen technische en organisatorische maatregelen ten spijt, het ontbreken van privacy awareness binnen een organisatie is een compliancerisico en heeft tot gevolg dat er een hoger risico is op het krijgen van een boete wanneer er bijvoorbeeld een datalek is of persoonsgegevens niet op de juiste wijze worden verwerkt (zie ook art. 83 lid 2 sub d AVG). Alle reden om binnen de organisatie de privacy awareness onder de medewerkers te vergroten en daar blijvend aandacht aan te besteden. Ten slotte kan worden opgemerkt dat de aanwezigheid van een privacy-awarenessbeleid bijdraagt aan het conform art. 5 lid 2 AVG ("accountability") aannemelijk maken dat wordt voldaan aan de verplichtingen, die op verwerkingsverantwoordelijke en verwerker berusten, om passende gegevensbeschermings- en beveiligingsmaatregelen te treffen (o.a. art. 24, 28 en 32 AVG).

Algemeen:

- ☐ kies een strategie die bij de organisatie past en zorg dat deze ook door de directie wordt uitgedragen ("tone at the top" is essentieel);
- ☐ maak duidelijk wie verantwoordelijk is voor de uitrol van privacy awareness;
- ☐ houd de boodschap simpel en begrijpelijk en maak de doelgroep specifiek (onderscheid management en werkvloer);
- ☐ boodschap kan variëren van een schriftelijke instructie (protocollen, intranet) tot persoonlijke trainingen en e-learningmodules;
- ☐ houd een overzicht bij van medewerkers die getraind zijn;
- ☐ zorg voor een getekende presentielijst;
- ☐ privacy awareness maakt onderdeel uit van overige technische en organisatorische maatregelen die door de organisatie genomen zijn, denk hierbij (niet-limitatief) aan bijvoorbeeld:
  - clean-deskbeleid;
  - laptop altijd meenemen, niet onbemand achterlaten;
  - privacyschermen voor medewerkers (bijvoorbeeld tijdens reizen met openbaar vervoer);
  - een wachtwoordenbeleid;
  - installeren van beveiligingsupdates;
  - privacygevoelige documenten op de juiste wijze vernietigen;
  - opnemen van geheimhoudingsverklaringen in arbeidsovereenkomsten;
- ☐ varieer en verras in aanpak. Ludieke acties (bijvoorbeeld een nep-phishingcampagne onder medewerkers kan het privacybewustzijn vergroten);
- ☐ belonen versus straffen. Bedenk op welke wijze het privacybewustzijn kracht bijgezet kan worden (bijvoorbeeld door het verstrekken van een boekenbon aan medewerkers die intern op de juiste wijze een datalek melden, of een traktatie voor een afdeling als beloning voor een positieve uitkomst van een privacyaudit versus een aantekening in het personeelsdossier);
- ☐ maak weerstand bespreekbaar;
- ☐ is er ruimte voor zelfreflectie;
- ☐ neem vaste verantwoordingsmomenten op (bijvoorbeeld tijdens jaargesprekken);
- ☐ kracht van de herhaling, besteed blijvend aandacht aan privacy awareness (naast het periodiek trainen en het verrichten van audits kan ook gedacht worden aan een FAQ-pagina op de intranetsite waar een overzicht staat van de meest gestelde vragen over privacy);
- ☐ breng privacy awareness onder de aandacht bij nieuwe medewerkers.

Overige aandachtspunten:

- ☐ het CIP *(Centrum voor Informatiebeveiliging en Privacybescherming) heeft verschillende documenten die nuttig kunnen zijn voor privacy awareness publiek beschikbaar gemaakt, zie:*
  - https://www.cip-overheid.nl/category/producten/awareness
  - https://www.cip-overheid.nl/category/workshops
- ☐ ook *via andere openbare bronnen als YouTube zijn awarenessvideo's beschikbaar die organisaties bereid zijn te delen. Dergelijke filmpjes kunnen onderdeel zijn van een awarenesstraining;*
- ☐ *de AVG verplicht de FG tot aandacht voor opleidingsactiviteiten (art. 39 lid 1 sub b AVG);*
- ☐ *in BCR dient het onderwerp "opleiding" te worden geadresseerd (art. 47 lid 2 sub h en n AVG).*

4 Voorbereiden organisatie

Bij het voorbereiden van de organisatie op de AVG is het wenselijk om een privacybeleid op te stellen. De directie dient daarbij te worden betrokken. Naleving van de privacywet- en regelgeving is een verantwoordelijkheid van de directie. Daarbij gelden de volgende aandachtspunten:

- ☐ agenderen AVG bij de directie;
- ☐ opstellen voorstel aanpak AVG;
- ☐ alloceren verantwoordelijkheid binnen de directie;
- ☐ aanwijzen projectleider implementatie;
- ☐ overwegen om een FG of een privacycoördinator aan te stellen;
- ☐ laten opstellen of herzien van policies klant/medewerker/burger;
- ☐ (opnieuw) opstellen van policy nieuwe ICT-projecten (verplicht gebruik Data Protection Impact Assessment (DPIA));
- ☐ (opnieuw) accorderen beveiligingsbeleid;
- ☐ Binding Corporate Rules (BCR) als aanpak voor multinational (ook voor verwerkers);
- ☐ bewustheid van de medewerkers binnen de organisatie als aandachtspunt (awarenessprogramma's);
- ☐ betrokkenheid OR als aandachtspunt;
- ☐ inregelen accountability (verantwoordingsbeginsel: zie WP 173. Zie ook art. 5 lid 2 jo. art. 24 lid 2 AVG).