Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Checklist nieuwe privacywet (AVG)

Wilt u uw organisatie voorbereiden op de nieuwe privacywetgeving, de Algemene Verordening Gegevensbescherming (AVG)? Hieronder staat een checklist van actiepunten waarmee u uw organisatie kunt voorbereiden op de nieuwe privacywet.

We hebben ook links gezet naar de documenten van Smith&Doe die uw organisatie daarbij kunnen helpen.

Let op: de privacy checklist is een algemene checklist. We raden aan om ook altijd het Ebook "In 8 stappen voorbereiden op de nieuwe privacywet" te bestellen. Daarin staan de te nemen stappen uitgebreider omschreven.

1. PAK HET AAN ALS EEN PROJECT

Zorg dat de voorbereidingen op de nieuwe privacywetgeving worden aangepakt als een project. Er moeten meestal meerdere stappen worden genomen, die tijd kosten. Benoem zo nodig iemand die het project leidt en een team dat meehelpt.

2. MAAK EEN INVENTARISATIE (“DATA-MAP”)

Stel vast welke persoonsgegevens uw organisatie gebruikt (“verwerkt”). Maak een overzicht van de gegevens.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

U kunt hiervoor onze tool Overzicht Gegevensstromen gebruiken. In ons blogbericht over het aanleggen van dit overzicht staat wat er verplicht in moet worden opgenomen.

3. CHECK: MOETEN WE EEN FG BENOEMEN?

Ga na of uw organisatie een Functionaris Gegevensbescherming moet benoemen.

Kijk hiervoor in het Factsheet FG.

Noot: in de privacyverklaring zullen de contactgegevens van de FG moeten worden opgenomen.

4. CHECK: GEBRUIKEN WE BIJZONDERE PERSOONSGEGEVENS?

Ga na of er door uw organisatie zogenaamde “bijzondere persoonsgegevens” worden gebruikt.

Kijk in ons Factsheet Bijzondere Persoonsgegevens om dit na te gaan. In principe geldt een verbod om dit soort persoonsgegevens te gebruiken, tenzij er sprake is van een wettelijke uitzondering. Raadpleeg eventueel een jurist.

Hoewel het niet wettelijk verplicht is, raden wij aan om in het Overzicht Gegevensstromen vast te leggen of er bijzondere persoonsgegevens worden gebruikt en zo ja, welke. Ook raden we aan om aan te geven op basis van welke wettelijke uitzondering de persoonsgegevens worden gebruikt.

5. CHECK: GEBRUIKEN WE PERSOONSGEGEVENS VAN KINDEREN?

Ga na of er binnen uw organisatie ook persoonsgegevens van kinderen – personen onder de 16 jaar – worden gebruikt.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Kijk in ons Factsheet Gegevens Kinderen voor meer informatie over welke specifieke regels hiervoor gelden. Neem de benodigde maatregelen om die regels op te volgen.

Hoewel het niet wettelijk verplicht is, raden wij aan om in het Overzicht Gegevensstromen vast te leggen dat er persoonsgegevens van kinderen worden verwerkt.

Noot: als uw organisatie zich richt op kinderen moet de privacyverklaring worden afgestemd op hun niveau.

6. BEPAAL DE DOELEINDEN

Bepaal waarvoor uw organisatie de persoonsgegevens verwerkt. Dit worden de “doeleinden” genoemd waarvoor uw organisatie de persoonsgegevens verwerkt.

Kijk in ons Dossier Doeleinden voor meer informatie over het vastleggen van de doeleinden.

Leg de doeleinden vast in het Overzicht Gegevensstromen. Dit is wettelijk verplicht.

Noot: de doeleinden moeten ook worden vastgelegd in de privacyverklaring.

7. CHECK: GEBRUIKEN WE NIE TE VEEL EN NIET TE WEINIG?

Ga na of uw organisatie niet te veel maar ook niet te weinig persoonsgegevens gebruikt.

Niet te veel:

Er mogen niet meer persoonsgegevens worden gebruikt dan nodig (noodzakelijk) is voor het doel waarvoor ze worden gebruikt.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Niet te weinig ("toereikend"):

Ook mogen er niet te weinig persoonsgegevens worden gebruikt. Dit betekent kort gezegd dat uw organisatie niet zo weinig informatie over de persoon mag hebben dat uw organisatie niet een juist of volledig beeld van hem of haar heeft. Dit gezien de doeleinden waarvoor de gegevens worden gebruikt.

> *Bijvoorbeeld: als een klant een factuur niet betaalt omdat hij de factuur inhoudelijk betwist, dan moet die inhoudelijke betwisting ook worden vastgelegd, anders krijgt u niet een volledig beeld van waarom de klant de factuur niet wil betalen.*

8. CONTROLEER DE RECHTSGROND / RECHTSGROND

Ga na of er voor ieder soort gebruik dat er van de persoonsgegevens wordt gemaakt een “rechtsgrond” (ook wel: “rechtsgrond”) is.

Kijk in ons Factsheet Rechtsgronden voor meer informatie. Ga daarmee ook na of de manier waarop toestemming wordt gevraagd voldoet aan de eisen die de nieuwe privacywet daaraan stelt.

Zonder een geldige rechtsgrond mag uw organisatie de persoonsgegevens niet verwerken.

Hoewel het niet wettelijk verplicht is, is het wel handig om de rechtsgronden in het Overzicht Gegevensstromen vast te leggen.

Noot: de rechtsgronden moeten ook worden omschreven in de privacyverklaring. Als uw organisatie zich beroept op het zogenaamde “gerechtvaardigde belang” dan moet ook worden omschreven wélke gerechtvaardigde belangen dat zijn.

Smith & Doe privacytools

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

9. CHECK: GEBRUIKEN WE UITSLUITEND GEAUTOMATISEERDE INDIVIDUELE BESLUITVORMING, WAARONDER PROFILING?

Ga na of er door uw organisatie gebruik wordt gemaakt van zogenaamde "uitsluitend geautomatiseerde individuele besluitvorming", waaronder profilering. Als dit soort besluitvorming, waaronder profilering "rechtsgevolgen" heeft voor de persoon of het de persoon op een andere manier in aanzienlijke mate treft, dan gelden daar specifieke regels voor.

Kijk in ons Factsheet Profiling voor meer informatie hierover. In het factsheet staat ook welke regels gelden in deze situatie. Neem de benodigde maatregelen om die regels op te volgen.

Hoewel het niet wettelijk verplicht is, is het wel handig om het Overzicht Gegevensstromen vast te leggen als er sprake is van uitsluitend geautomatiseerde individuele besluitvorming, waaronder profilering, waar de specifieke regels voor gelden.

Noot: in de privacyverklaring moet worden aangegeven of er gebruik wordt gemaakt van dit soort besluitvorming, wat het belang en de gevolgen daarvan zijn voor de betrokken personen en de logica erachter.

10. CHECK: VAN WIE ONTVANGEN WIJ PERSOONSGEGEVENS?

Ga na van welke andere organisaties uw organisatie persoonsgegevens ontvangt.

Hoewel het niet wettelijk verplicht is, raden we aan om in het Overzicht Gegevensstromen vast te leggen van welke organisaties uw organisatie de persoonsgegevens ontvangt. Dit is de "herkomst" van de persoonsgegevens.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Noot: Voor de persoonsgegevens die u van een andere partij ontvangt, moet in de privacyverklaring worden aangegeven welke persoonsgegevens dat zijn en wat de herkomst (bron) daarvan is.

11. CHECK: AAN WIE GEVEN WIJ PERSOONSGEGEVENS DOOR?

Ga na aan welke externe personen of partijen uw organisatie de persoonsgegevens doorgeeft.

Ga ook na welke externe personen of partijen in opdracht van uw organisatie handelingen verrichten met de persoonsgegevens, bijvoorbeeld het inzien, opslaan, verwijderen of doorgeven. Dit soort personen of partijen worden verwerkers genoemd.

Beide soorten externe personen of partijen worden “ontvangers” genoemd.

Leg in het Overzicht Gegevensstromen vast welke soorten ontvangers er zijn. Dit is wettelijk verplicht.

Geef de gegevens niet zomaar door aan andere partijen. Als u twijfelt of u gegevens door mag geven aan een andere partij, neem dan contact op met een privacy-jurist en vraag naar de mogelijkheden.

12. SLUIT VERWERKERSOVEREENKOMSTEN AF

Sluit verwerkersovereenkomsten af met externe leveranciers (verwerkers).

Kijk voor meer informatie over verwerkers in ons Dossier verwerkers.

U kunt hiervoor de volgende verwerkersovereenkomsten bestellen:

Verwerkersovereenkomst Dienstverleners AVG
Verwerkersovereenkomst Hosting AVG

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Verwerkersovereenkomst Cloud AVG
Eenvoudige verwerkersovereenkomst ZZP-ers AVG

13. SLUIT OVEREENKOMSTEN AF MET ANDERE VERANTWOORDELIJKEN

Is uw organisatie samen met een of meer andere externe partijen verantwoordelijk voor dezelfde set persoonsgegevens? Dat is het geval als u en die andere partij(en) bepalen dát de persoonsgegevens worden verwerkt, waarvoor dat gebeurt en hoe.

In de privacywet wordt dit het “bepalen van het doel en de middelen” van de verwerking van de persoonsgegevens genoemd.

Met dit soort externe partijen moet een overeenkomst worden gesloten.

U kunt hiervoor een Overeenkomst Verantwoordelijken bestellen.

In het Overzicht Gegevensstromen moeten de naam en contactgegevens van de andere verantwoordelijken vast worden gelegd. Dit is wettelijk verplicht.

Noot: in de privacyverklaring moet worden aangegeven aan welk partijen, of als dat niet kan, aan welk soort partijen de gegevens worden doorgegeven. Dat geldt niet alleen voor andere marktpartijen en andere verantwoordelijken, maar ook verwerkers, overheidsinstanties en groepsmaatschappijen.

14. EXPORTEER DATA ALLEEN NAAR BUITEN DE EER ALS DAT MAG

Ga na waar de persoonsgegevens worden opgeslagen, daarmee bedoelen we: in welk(e) land(en). Ga na bij uw IT-dienstverleners en

Smith & Doe privacytools

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

andere verwerkers waar zij gevestigd zijn en waar zij de persoonsgegevens opslaan. Controleer dit ook voor internetapplicaties waar persoonsgegevens in worden verwerkt (geupload): welke partijen bieden deze aan? Waar slaan zij de persoonsgegevens op?

Ga ook na vanuit welk(e) land(en) personen toegang hebben tot persoonsgegevens, als dat bijvoorbeeld via het internet is.

Ga na of de persoonsgegevens worden opgeslagen door, doorgegeven aan of toegankelijk zijn voor partijen die zich buiten de EER (de EU landen, Noorwegen, Liechtenstein en IJsland) bevinden.

In principe geldt er een verbod om persoonsgegevens door te geven naar buiten de EER. Maar in de wet staan uitzonderingen. Kijk hiervoor in het Factsheet Dataexport.

Neem als dat nodig is, maatregelen om te zorgen voor geldige doorgifte naar buiten de EER. Eén van de mogelijk maatregelen is het afsluiten van een "Modelcontract van de EU".

U kunt bij ons een Modelcontract van de Europese Unie bestellen.

Het is wettelijk verplicht om in het Overzicht Gegevensstromen vast te leggen dat persoonsgegevens naar buiten de EER worden doorgegeven, naar welk land en als de persoonsgegevens worden doorgegeven op basis van zogenaamde "bijzondere omstandigheden" (kijk voor een uitleg hierover in ons Factsheet Dataexport), de relevante documenten met betrekking tot de passende waarborgen.

Smith & Doe privacytools

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Noot: in de privacyverklaring moet ook worden aangegeven of de persoonsgegevens worden doorgegeven naar buiten de EER en welke "passende waarborgen" er zijn voor doorgifte.

15. VERPLICHT MEDEWERKERS TOT GEHEIMHOUDING

Verplicht de eigen medewerkers die met de persoonsgegevens werken tot geheimhouding daarvan en het alleen verwerken van de persoonsgegevens in het kader van hun werkzaamheden.

U kunt hiervoor een Geheimhoudingsverklaring bestellen.

16. ZORG VOOR DATAKWALITEIT

Zorg dat de gegevens juist, compleet en up to date zijn. Dit is vooral relevant bij databases met persoonsgegevens.

17. BEWAAR NIET LANGER DAN NODIG

Zorg dat de gegevens niet langer worden bewaard dan noodzakelijk voor het doel waarvoor ze zijn verzameld. Als uw organisatie veel persoonsgegevens verwerkt, is het aan te raden om bewaartermijnen protocollen te maken.

De AVG schrijft voor dat in het Overzicht Gegevensstromen, “indien mogelijk” de bewaartermijnen moeten worden opgenomen.

Noot: in de privacyverklaring zal moeten worden aangegeven hoe lang de gegevens worden bewaard of wat de bewaarcriteria zijn.

18. VOER PIA’s UIT (ALS DAT NODIG IS)

Voer, als dat verplicht is, privacy impact assessments (PIA’s) uit.

Ga met ons Factsheet PIA’s na wanneer PIA’s verplicht zijn.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

We zullen in de loop van 2017-2018 een PIA toevoegen aan onze website. Als u hierover wilt worden geïnformeerd, meld u dan aan voor de Privacy Alert.

Hoewel het niet wettelijk verplicht is, raden we aan om in het Overzicht Gegevensstromen aan te geven of er een PIA is uitgevoerd voor de betreffende "stroom" persoonsgegevens.

19. PAS WAAR MOGELIJK PRIVACY BY DESIGN EN BY DEFAULT TOE

Neem, (kort gezegd:) waar dat mogelijk en toepasselijk is, passende technische en organisatorische maatregelen om "privacy by design" en "privacy by default" toe te passen op de "stromen" persoonsgegevens.

Privacy by design houdt kort gezegd in dat uw organisatie onderzoekt op welke manier de privacyregels feitelijk en technisch kunnen worden toegepast en welke maatregelen kunnen worden genomen om de rechten van de betrokken personen te beschermen.

> *In de AVG worden als voorbeelden gegeven: pseudonimiseren en het minimaliseren van de hoeveelheid persoonsgegevens.*

Privacy by default houdt kort gezegd in dat uw organisatie technische en organisatorische maatregelen neemt om te zorgen dat alleen persoonsgegevens worden gebruikt die noodzakelijk zijn voor de doeleinden waarvoor ze worden verzameld. Dit slaat op de hoeveelheid persoonsgegevens, de omvang van het gebruik en hoe lang de persoonsgegevens worden opgeslagen.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

De AVG noemt als voorbeeld dat persoonsgegevens niet beschikbaar worden gesteld aan een onbeperkt publiek (bijvoorbeeld via het internet) zonder tussenkomst van de betrokken persoon.

20. ZORG VOOR PASSENDE BEVEILIGING

Zorg voor passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen. De privacy-toezichthouder (de Autoriteit Persoonsgegevens) heeft hiervoor Beveiligingsrichtsnoeren gepubliceerd.

De AVG schrijft voor dat in het Overzicht Gegevensstromen, “indien mogelijk” een algemene omschrijving moet worden gegeven van de beveiligingsmaatregelen.

21. MELD DATALEKKEN WANNEER DAT MOET

Meld datalekken aan de privacy-toezichthouder (de Autoriteit Persoonsgegevens) en de betrokken personen om wiens gegevens het gaat, als dat moet.

In onze webshop bieden wij hiervoor een Draaiboek Datalekken op basis van de AVG aan.

22. WEES TRANSPARANT (UPDATE DE PRIVACYVERKLARING)

Informeer mensen over wat u met de persoonsgegevens doet. Dit kan in een privacyverklaring.

Hoewel het niet wettelijk verplicht is, raden we aan om in het Overzicht Gegevensstromen aan te geven welke privacyverklaring er geldt voor de betreffende “stroom” persoonsgegevens, met waar mogelijk hyperlinks daarnaar.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

23. VOLDOE AAN DE RECHTEN VAN BETROKKENEN

Voldoe aan de rechten van de personen wiens gegevens u verwerkt.

Kijk voor meer informatie in ons Factsheet Verzoeken.

Zorg dat het "recht op overdraagbaarheid" van de persoonsgegevens wordt gefaciliteerd. In bepaalde gevallen hebben de betrokken personen recht op overdracht van hun persoonsgegevens, kijk hiervoor in het Factsheet verzoeken.

Wij hebben een Draaiboek (protocol) Verzoeken Betrokkenen gemaakt die uw organisatie kan ondersteunen bij het in behandeling nemen van de verzoeken.

Noot: in de privacyverklaring moeten de rechten van de betrokkenen worden omschreven.

24. MAAK DE BENODIGDE DOCUMENTEN

Maak de verschillende documenten om de privacy-compliance te ondersteunen. Zie de documenten die we hiervoor hebben genoemd, maar denk ook aan een beveiligingsbeleid en specifieke protocollen, zoals bijvoorbeeld een cameraprotocol.

Wij hebben ook een algemeen Privacy-beleid om te gebruiken als basis voor het beleid dat uw organisatie voert met betrekking tot persoonsgegevens.

25. RICHT (WAAR NODIG) PROCESSEN IN

Met “processen inrichten” doelen we op het creëren van processen binnen de organisatie om de privacy-compliance te ondersteunen.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Dit geldt vooral voor organisaties waar meerdere medewerkers werken.

Denk bijvoorbeeld aan de volgende processen:

- Proces rondom nieuwe projecten;
- Proces bij nieuwe onderaannemers (verwerkers);
- Proces bij “uitsluitend geautomatiseerde individuele beslissingen”;
- Proces rondom kwaliteit van de gegevens;
- Proces rond datalekken;
- Proces rond het bewaren van persoonsgegevens;
- Proces rond het voldoen aan de verzoeken van betrokken personen, waaronder overdracht van de persoonsgegevens aan de betrokken persoon.

26. RICHT EEN INTERN INFORMATIEPUNT IN

Richt een “intern loket” in waar de medewerkers van uw organisatie met hun privacy-vragen terecht kunnen. Met een “intern loket” bedoelen we het aanwijzen van een persoon die, of team dat privacy gerelateerde vragen van medewerkers binnen uw organisatie kan beantwoorden. Dit geldt voor organisaties waar meerdere medewerkers werken.

Maak de contactgegevens van het "interne loket" bekend binnen de organisatie.

27. RICHT EEN EXTERN INFORMATIEPUNT IN

Richt ook een “extern informatiepunt” in waar de betrokken personen terecht kunnen met vragen over hun persoonsgegevens.

Zuid-Hollandlaan 7
2596 AL Den Haag
070 324 35 89
Info@smithanddoe.com
www.smithanddoe.com
www.privacytools.nl

Het is aan te raden om het informatiepunt ook de verzoeken van de betrokken personen in behandeling te laten nemen waarbij de betrokken personen hun “rechten” uitoefenen (zie punt 21).

Noot: de contactgegevens van het informatiepunt neemt u op in de privacyverklaring.

28. INFORMEER EN TRAIN DE ORGANISATIE

Hierbij gaat het om het creëren van “awareness” binnen de organisatie over wat wel en niet met de persoonsgegevens mag worden gedaan en welke documenten er zijn om de privacy-compliance te ondersteunen. Dit geldt voor organisaties waar meerdere medewerkers werken.

Daarnaast zullen de medewerkers die met de persoonsgegevens werken moeten worden getraind op privacy-compliance, waar nodig op specifieke onderwerpen.

Wij geven in house trainingen. Neem contact op een vraag naar de mogelijkheden.