Hunter Management Partners BV

Bezoekadres:
Lopikerplein 2a, Schoonhoven
2e etage "De Toren"

Postadres:
Postbus 9, 3410 CA Lopik

Tel: 0182 - 389036
Fax: 0182 - 389048
E-mail: hmp@hmp.nl
Web: www.hmp.nl
KvK Midden NL 53164946

PRIORITEITENOVERZICHT AVG

Om te voldoen aan de AVG op 25 mei 2018, dient u als organisatie meerdere stappen te ondernemen. Door de hoeveelheid informatie, nieuwsbrieven en seminars, ziet u wellicht door de bomen het bos niet meer.

De verschillende checklisten van Hunter Management Partners geven u al een goed overzicht van de stappen die doorlopen moeten worden om te voldoen aan de AVG. De checklisten staan daarnaast vol met nuttige, praktische informatie en uitvoeringsrichtlijnen.

Dit prioriteitenoverzicht is bedoeld om aan te geven welke onderwerpen in welke volgorde opgepakt moeten worden. Op 25 mei 2018 dient u te voldoen aan de AVG en vanaf deze datum kan de Autoriteit Persoonsgegevens u een boete opleggen voor het niet voldoen aan de wetgeving. We hebben namelijk al vanaf de datum van inwerkingtreding van de AVG in 2016, de tijd gehad om de wijzigingen door te voeren.

Vragen of wilt u weten wat Hunter Management Partners voor u kunt betekenen betreffende de vernieuwde privacywetgeving? *Neem contact op met mr. V.S. (Vera) Verlooij, junior partner en jurist bij HMP, via v.verlooij@hmp.nl.*

CHECKLIST

- ☐ Register verwerkingsactiviteiten
- ☐ Privacyverklaring updaten
- ☐ Cookieverklaring updaten
- ☐ Verwijzen op website naar privacyverklaring
- ☐ Controleer checkboxen website
- ☐ Cookietoestemming website
- ☐ Register verwerkingsactiviteiten
- ☐ Bepaal en stel aan FG
- ☐ Bepaal en voer uit DPIA
- ☐ Beveiliging aanpassen
- ☐ Verwerkersovereenkomsten opstellen
- ☐ Datalek beleid
- ☐ Privacybeleid
- ☐ Opruimen persoonsgegevens

Prioriteit 1: Maak uw website AVG-proof
Toelichting: Uw website is uw voordeur. Mocht de Autoriteit Persoonsgegevens een klacht ontvangen over uw organisatie, dan lijkt me de kans zeer groot dat de Autoriteit begint met het bekijken van de website. Voldoet de website al niet aan de AVG, dan is de kans groot dat de regelgeving intern ook niet voldoet.
Uitvoering: - Stel een nieuwe privacyverklaring op, die voldoet aan de vereisten van de AVG; - Verwijs bij contactformulieren, nieuwsbriefinschrijvingsformulieren e.d. naar de privacyverklaring; - Controleer of checkboxen niet vooraf zijn aangevinkt; - Pas de cookie toestemming, waar nodig volgens de AVG, aan.

Prioriteit 2: Start met het register van verwerkingsactiviteiten
Toelichting: Het register is de basis van alle overige stappen en maatregelen. Zonder dat er in kaart is gebracht hoe de verwerking van persoonsgegevens binnen de organisatie plaatsvindt, kan er bijvoorbeeld geen privacyverklaring opgesteld worden en is niet duidelijk of er veel bijzondere persoonsgegevens verwerkt worden. Het register is daarnaast het werkdocument voor de AVG. Constant worden hierop gegevens aangevuld, aangepast en verwijderd.
Uitvoering: Maak in het verwerkingsactiviteitenregister alvast een inventarisatie van de antwoorden op de volgende vragen: - Van welke categorie personen verzamelt de organisatie gegevens? (klanten, potentiële klanten, leveranciers, werknemers) - Welke persoonsgegevens verzamelt de organisatie? (bijvoorbeeld, naam, telefoonnummer) - Verzamelt de organisatie ook bijzondere persoonsgegevens? (BSN, NAW gegevens, pasfoto's, camerabeelden) - Met welk doel en met welke grondslag worden de persoonsgegevens verwerkt? (marketing, overeenkomst, verplicht vanuit andere instanties zoals de Belastingdienst) - Worden de persoonsgegevens gedeeld met andere (internationale) organisaties?

Prioriteit 3: Bepaal of een FG en een DPIA nodig zijn
Toelichting: Voor het aanstellen van een Functionaris Gegevensbescherming of het uitvoeren van een DPIA, kan u wettelijk verplicht zijn. Stel dit vast. Wanneer onduidelijk is of uw organisatie verplicht is om een FG aan te stellen, onderbouw goed waarom wel of niet gekozen is voor het aanstellen van een FG. Neem de benodigde maatregelen als vast komt te staan dat uw organisatie een deze verplichtingen moet voldoen.

Prioriteit 4: Beveiligen

Toelichting:
Vanzelfsprekend is het beveiligen van persoonsgegevens een van de belangrijkste onderdelen van de AVG. Neem daarom zo snel mogelijk en waar mogelijk de benodigde technische maatregelen, zoals:

- Up-to-date houden van software;
- Back-up maken en deze veilig opslaan;
- Versleutelen van gegevens,
- Verwijderen van verouderde gegevens;
- Goede toegangsbeveiliging: bijvoorbeeld 2-staps verificatie;
- Installeren van een virusscanner en firewall.

Prioriteit 5: Stel verwerkersovereenkomsten op

Toelichting:
Als een organisatie gegevensverwerking uitbesteed, dient met deze verwerker een verwerkingsovereenkomst opgesteld te worden.

Een verwerker is een persoon of organisatie die in opdracht van jou werkt met jouw verzamelde persoonsgegevens maar niet zelfstandig verantwoordelijk is voor de verwerking van de persoonsgegevens (over deze gegevens geen beslissingen mag maken). Denk aan de salarisadministratie, software, hosting partijen, (Cloud) opslag e.d.

Uitvoering:

1. Maak een overzichtslijst van alle derden die u inhuurt voor de verwerking van persoonsgegevens.
2. Stel met iedere verwerker een verwerkingsovereenkomst op of inventariseer of deze door de verwerker zelf beschikbaar is gesteld.
3. Documenteer de lijst met verwerkers en de bijbehorende verwerkingsovereenkomsten.

Prioriteit 6: Werk het verwerkingsactiviteitenregister verder uit

Toelichting:
Het verwerkingsregister mist nog enkele gegevens:

- De bewaartermijnen;
- Wie de gegevens intern verzamelen;
- Wie er toegang heeft tot de gegevens;
- Hoe de gegevens beveiligd zijn;

Uitvoering:

1. Bepaal als organisatie of een DPIA verplicht is;
2. Zo ja, voer de beoordeling uit volgens de richtlijnen van de Autoriteit Persoonsgegevens.

Prioriteit 7: Datalek, beleid en datalekregister

1. Stel een datalekbeleid op.

- Maak het intern duidelijk wat een datalek is en hoe deze intern gemeld moet worden en bij wie.
- Stel een stappenplan datalek op. Datalekken moeten zo spoedig mogelijk maar uiterlijk binnen 72 uur gemeld worden.

2. Stel een datalekregister op: alle datalekken binnen de organisatie moeten worden vastgelegd in een register. Hierin moet worden opgenomen:

- Het soort gegevens
- Een omschrijving van het datalek
- Wanneer het datalek plaats vond;
- Wat er met de persoonsgegevens gebeurd is;
- Van welke personen gegevens gelekt zijn;
- Of er melding gemaakt is van het datalek;
- Binnen hoeveel uur het datalek gemeld is.

Prioriteit 8: Privacy beleid

Nu het verwerkingsactiviteitenregister compleet is, is overzichtelijk hoe de gegevensverwerking intern verloopt. Vanuit deze informatie kan een intern privacy beleid opgesteld worden.

Prioriteit 9: Opruimen

Alle stappen van de checklist zijn doorlopen, met uitzondering van het opruimen van bestaande persoonsgegevens.
Duidelijk is geworden hoe de gegevensverwerking eruit hoort te zien. Nu is het zaak om de werkelijkheid aan te passen op de interne AVG richtlijnen. Dat betekent alle onnodige, overbodige, niet toegestane en incorrecte gegevens verwijderen.

Disclaimer
Hunter Management Partners heeft zijn best gedaan om zich zo goed mogelijk te verdiepen in de nieuwe wetgeving en de regels zo helder mogelijk aan u uit te leggen. Desondanks kan het zijn dat er onverhoopt toch onjuiste of onvolledige informatie in deze checklist is geslopen. Zie u iets dat niet klopt of niet duidelijk is? Laat het ons weten via e-mail: hmp@hmp.nl of telefonisch 0182-389036