Stappenplan AVG

Hoe voldoe ik aan de nieuwe privacyverordening?

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. Door de nieuwe privacywet krijgt u meer verplichtingen, krijgen betrokkenen meer rechten, heeft de nationale toezichthouder, de Autoriteit Persoonsgegevens (AP), meer bevoegdheden en mogen hogere boetes worden opgelegd.

Hieronder laten wij zien hoe u in negen stappen voldoet aan de AVG.

Stap 1. Bewustwording

Draag uit dat de organisatie de privacy van personen wil respecteren. Geef voorlichting binnen uw organisatie over de verwerking van persoonsgegevens.

Maak een of meerdere personen verantwoordelijk binnen de organisatie voor de bescherming van persoonsgegevens en bepaal of u een functionaris voor de gegevensbescherming (**FG**) aanstelt (mogelijk is dit zelfs verplicht). Meer informatie over de FG vindt u op de site van de Autoriteit Persoonsgegevens.

Maak gebruik van de informatie op de website van de Autoriteit Persoonsgegevens en het ABU-ledennet. Op het ledennet vindt u documenten die bij de vervolgstappen behulpzaam kunnen zijn, zoals de Handreiking do's en don'ts en de FAQ's.

Stap 2. Overzicht van de persoonsgegevens die u verwerkt

Breng alle verwerkingen van persoonsgegevens binnen uw organisatie in kaart en leg dit vast in een **verwerkingsregister**. U kunt gebruikmaken van het model verwerkingsregister en de toelichting op dit model op het ABU-ledennet. Meer informatie over het verwerkingsregister vindt u op de site van de Autoriteit Persoonsgegevens.

Stel vast en registreer in het verwerkingsregister op basis van welke **wettelijke grondslag** het verwerken van persoonsgegevens plaatsvindt.

De zes wettelijke grondslagen zijn:
- toestemming van de betrokkene*;
- noodzakelijk voor het uitvoeren van een overeenkomst;
- noodzakelijk voor de uitvoering van een wettelijke verplichting;
- vitaal belang van de betrokkene;
- uitvoeren van een publiekrechtelijke taak;
- gerechtvaardigd belang van de organisatie.

* Let op bij 'toestemming van de betrokkene'. Doordat er tussen werknemer en werkgever een afhankelijkheidsrelatie bestaat, kan de werknemer in beginsel de werkgever geen toestemming geven om persoonsgegevens te verwerken. In deze verhouding kan de toestemming namelijk vaak niet als in vrijheid gegeven worden beschouwd.

Bepaal ook of de persoonsgegevens daadwerkelijk worden verwerkt in overeenstemming met het **doel** waarvoor ze zijn verkregen. Meer informatie over de wettelijke grondslagen en doelen vindt u op de site van de Autoriteit Persoonsgegevens.

Controleer extra kritisch of uw organisatie **bijzondere persoonsgegevens** verwerkt in overeenstemming met de wet. Bijzondere persoonsgegevens zijn gegevens waaruit iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, gezondheid, strafrechtelijk gedrag, seksuele leven of het lidmaatschap van een vakbond blijken. Ook genetische gegevens en biometrische gegevens voor unieke identificatie van een persoon vallen hieronder.
De verwerking van bijzondere persoonsgegevens is verboden, tenzij een wettelijke uitzondering van toepassing is en het strikt noodzakelijk is om ze hiervoor te verwerken. Op de site van de Autoriteit Persoonsgegevens vindt u een overzicht van wanneer u bijzondere persoonsgegevens mag verwerken.

Ook het verwerken van het **burgerservicenummer** verdient extra aandacht. Meer hierover op de site van de Autoriteit Persoonsgegevens.

Stap 3. Rechten van betrokkenen

Informeer de betrokkene voordat u persoonsgegevens verwerkt over welke persoonsgegevens worden verwerkt, het doel van de verwerking, de ontvangers van de gegevens, hoe lang de gegevens worden bewaard, hoe de gegevens zijn beveiligd en welke rechten de betrokkene heeft. Deze informatie kan in een **privacystatement** worden opgenomen.
Dit privacystatement kunt u op uw website plaatsen. De voorwaarden waaraan het

privacystatement moet voldoen, kunt u vinden in artikel 12, 13 en 14 van de AVG.

Onder de AVG hebben betrokkenen **meer en verbeterde privacyrechten**. Zij kunnen verzoeken om inzage, correctie, verwijdering en dataportabiliteit. Zorg dat uw organisatie hierop is voorbereid. Meer informatie over deze privacyrechten vindt u op de site van de Autoriteit Persoonsgegevens.

Stap 4. Beveiligingsmaatregelen

Stel **informatiebeveiligingsbeleid** vast en maak dit bekend binnen de organisatie. In het beleid kunt u opnemen hoe apparatuur, omgeving, toegang, informatiesystemen (software) zijn beveiligd en hoe medewerkers hiermee moeten omgaan. Maak gebruik van gangbare beveiligingsmaatregelen zoals 'logging' en 'meerfactorauthenticatie'. Meer informatie over beveiligingsmaatregelen vindt u op de site van de Autoriteit Persoonsgegevens. U vindt hier ook veel gestelde vragen en antwoorden.

Stel een procedure op voor het omgaan met **datalekken** binnen de organisatie. U moet alle datalekken documenteren en in bepaalde gevallen melden bij de Autoriteit Persoonsgegevens en de betrokkenen. Meer informatie over datalekken vindt u op de site van de Autoriteit Persoonsgegevens.

Bepaal of u zich wilt verzekeren tegen de gevolgen van beveiligingsincidenten en datalekken en sluit, indien gewenst, een verzekering af.

U kunt bij het **opstellen van het informatiebeveiligingsbeleid** gebruikmaken van de Checklist beveiligingsmaatregelen op het ABU-ledennet.

Stap 5. Verwerkers en verwerkersovereenkomsten

Stel vast welke 'verwerkers' uw organisatie inschakelt (dienstverleners die in uw opdracht persoonsgegevens verwerken, zoals uw softwareleverancier).
Sluit **verwerkersovereenkomsten** met de verwerkers. Neem hierin onder andere op dat verwerking van persoonsgegevens alleen in opdracht van de verwerkingsverantwoordelijke kan plaatsvinden. Leg verder ook de beveiliging, geheimhouding en controlebevoegdheid van de verwerkingsverantwoordelijke hierin vast. U kunt gebruikmaken van de model verwerkersovereenkomst en de toelichting op dit model op het ABU-ledennet.

Stap 6. Bewaren en vernietigen

Organiseer binnen uw organisatie dat de regels over het bewaren en vernietigen van persoonsgegevens worden nageleefd. Denk hierbij aan de persoonsgegevens die voorkomen in de diverse systemen, e-mailboxen, etc. Per type persoonsgegeven gelden andere regels. Zie voor de verschillende bewaartermijnen het document bewaartermijnen op het ABU-ledennet.

Stap 7. Data Protection Impact Assessment (DPIA)

Als u persoonsgegevens gaat verwerken met een hoog privacyrisico, moet u eerst een **DPIA** uitvoeren. Denk bijvoorbeeld aan het gebruik van nieuwe verwerkingen of systemen waarin u bijzondere persoonsgegevens verwerkt of systemen die u gebruikt voor profilering van personen. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken. Meer informatie over de DPIA vindt u op de site van de Autoriteit Persoonsgegevens.

Op het ABU-ledennet vindt u een model DPIA dat u kunt gebruiken.

Stap 8. Privacy by design & privacy by default

Maak uw organisatie vertrouwd met de onder de AVG verplichte uitgangspunten van *privacy by design* en *privacy by default*, die gelden bij de ontwikkeling van nieuwe diensten.

Meer informatie en uitleg over deze begrippen vindt u op de site van de Autoriteit Persoonsgegevens.

Stap 9. Controle en evaluatie

Controleer regelmatig de naleving van maatregelen voor privacybescherming binnen de organisatie.

Zorg dat u op de hoogte blijft van nieuwe ontwikkelingen binnen het privacyrecht en pas zonodig de werkwijze aan.

Heeft u nog vragen?
Met vragen kunt u terecht bij de ABU-Helpdesk via helpdesk@abu.nl of
020 - 655 82 30 (9.00 - 12.30 uur) of uw eigen juridisch adviseur.