Compliance aan de Algemene Verordening Gegevensbescherming vraagt een antwoord op de volgende punten.

Neem hierbij de 'primaire uitgangspunten' vanuit het document "Infosheet AVG-compliance (GDPR)" in acht.

1. Stel register van verwerkingen op

U bent verplicht om met een register te werken waarin u de verwerking van persoonsgegevens bijhoudt, als één van de volgende punten van toepassing is:

- De organisatie is groter dan 250 medewerkers;
- De organisatie is kleiner dan 250 medewerkers maar u verwerkt persoonsgegevens:
  - die een hoog risico inhouden voor de rechten en vrijheden van de personen van wie u persoonsgegevens verwerkt *en/of;*
  - waarvan de verwerking niet incidenteel is *en/of*;
  - die vallen onder de categorie 'bijzondere persoonsgegevens', zoals gegevens over ras, BSN, gezondheid, strafrechtelijk verleden of politieke opvattingen;

U dient de kwaliteit van de persoonsgegevens te waarborgen door te bepalen aan welke kwaliteitseisen een verwerking moet voldoen en hier de benodigde maatregelen voor te treffen. Kwaliteitseisen dienen zoveel mogelijk via de functionaliteit van een informatiesysteem afgedwongen te worden.

2. Maak je risicomanagement inzichtelijk

De basis staat al benoemd in het 'register van verwerkingen' zoals aanwezige data. In het risicomanagement-document benoemen we dan ook meer specifiek de risico's en maatregelen.

Denk aan de volgende type maatregelen:

- Preventieve maatregelen: dienen te zijn ingericht om te voorkomen dat een dreiging leidt tot een beveiligingsincident.
- Detectieve maatregelen te zijn ingericht om te constateren dat een beveiligingsincident heeft plaatsgevonden.
- Voor het reduceren van de gevolgen van beveiligingsincidenten kunnen daarnaast repressieve en herstelmaatregelen ingericht worden.
- Correctieve maatregelen kunnen u helpen de gebleken tekortkomingen in de beveiliging te repareren.

Denk bij je omgevingen, met name bij ontwikkelen van nieuwe werkomgeving, aan:

- 'Privacy by design': vanuit ontwerp gegevens goed beschermen;
- 'Privacy by default': technische en organisatorische maatregelen nemen om 'als standaard' niet meer gegevens te ontvangen dan noodzakelijk is (een spelletjes-app op je telefoon niet de toegang tot de contacten of cameratoegang laten hebben.)

3. Verwerkersovereenkomsten

Regel de verantwoordelijkheden met externe partijen. Dit is een doorzetting van risicomanagement / zorgplicht naar de partijen die zaken voor jullie als verantwoordelijke uitvoeren.
Een aparte verwerkersovereenkomst is niet verplicht, de relevante onderwerpen mogen ook vastgelegd / afgetikt worden in het algemene contract of voorwaarden.

Als er gegevens buiten de EU worden opgeslagen, beoordeel dan of hiervoor een goede onderbouwing aanwezig is en zorg extra voor borging van een passend beschermingsniveau.

4. Uitvoeren DPIA (data privacy impact assessment)

Wanneer het verwerken van persoonsgegevens, in het bijzonder met behulp van nieuwe technologieën, (buitensporige) risico's voor betrokkenen inhoudt, is het uitvoeren van een PIA verplicht. Een PIA is in ieder geval verplicht bij:

- op grote schaal* bijzondere persoonsgegevens als ras, godsdienst, gezondheid, politieke opvattingen, genetische – of biometrische gegevens verwerkt;
- op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied, bijvoorbeeld met cameratoezicht;
- gegevens zo combineert, dat iemand in een bepaalde categorie of groep is in te delen en daardoor zo kan worden benaderd of beoordeeld (systematisch en uitvoering, waaronder profilering).

** Europese toezichthouders geven in 'Guidelines on Data Protection Officers' een aantal voorbeelden van wat zij als grootschalig zien:*

- *Een ziekenhuis dat patiëntgegevens verwerkt*
- *Een vervoersmaatschappij die reisinformatie verwerkt (bijvoorbeeld door reizigers te volgen via vervoerskaarten).*
- *Een verwerker die gespecialiseerd is in marktonderzoek en voor een klant de actuele locatiegegevens van hun klanten verwerkt voor statistische doeleinden.*
- *Een verzekeringsmaatschappij of bank die klantgegevens verwerkt*
- *Een zoekmachine die persoonsgegevens verwerkt om advertenties te kunnen tonen op basis van internetgedrag.*

Via een DPIA onderzoek je de impact en risico's van een bepaalde manier van verwerken van persoonsgegevens op de privacy van de betrokkenen en of je dit risico en impact kunt verlagen.
In sommige gevallen is het verplicht de PIA met betrokkenen te bespreken.
Vraag vrijblijvend naar deze AVG-werkwijze incl. DPIA-rapportage sjabloon.

Blijft het risico na maatregelen nog steeds hoog, dan moet je met de AP overleggen alvorens te starten met deze verwerking.

5. Beleg verantwoordelijkheid: een FG, PO, DPO of IB-verantwoordelijke

De functionaris voor gegevensbescherming, privacy officer, data protection officer, informatiebeveiligingsverantwoordelijke is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.

Een FG is in 3 situaties verplicht voor (art 37 van de AVG):

- overheidsinstanties en publieke organisaties. Denk aan rijksoverheid, gemeenten en provincies, maar ook bijvoorbeeld zorg- en onderwijsinstellingen. Voor rechtbanken geldt de verplichte aanstelling van een FG niet;
- organisaties die vanuit hun kernactiviteiten op grote schaal* individuen volgen. Het kan hierbij gaan om bijvoorbeeld profilering van mensen voor het maken van risico-inschattingen, cameratoezicht en monitoring van iemands gezondheid via *wearables*.
  ** Relevant hierbij is het aantal mensen (>5000), de hoeveelheid gegevens die de organisatie verwerkt en hoe lang organisatie mensen volgt.*
- organisaties die op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden.

EU-lidstaten kunnen ook andere situaties benoemen waarin een FG verplicht is. Het is nog niet bekend of dit in Nederland gaat gebeuren.

De functionaris moet onafhankelijk kunnen functioneren als privacy vraagbaak en mag zowel intern als extern aangesteld worden.
Je moet als organisatie kunnen onderbouwen waarom u wel of niet een FG hebt aangesteld.
Zie ook https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/functionaris-voor-de-gegevensbescherming-fg

6. Kennis en bewustwording

Zorg voor interne kennis en awareness, bijvoorbeeld door het geven van een presentatie/informatiesessie aan de medewerkers.
Denk aan het belang van IB, wetgeving, duidelijke werkwijze/huisregels.
Voorbeeld zie de posters, presentatie 'Bewustwording IB en AVG.pptx' en 'Dxx.Huisreglement informatiebeveiliging'.

7. Meldplicht datalekken en de AVG: eigen registratie van datalekken

Implementeer een procedure 'meldplicht datalekken' en zorg tevens voor interne registratie van inbreuken.
Je moet datalekken melden waarbij het 'waarschijnlijk is dat de betrokkene enige vorm van schade zal leiden'.
Je kunt hier dus ook denken aan procedures of systemen om datalekken of inbraken op een systeem op te sporen (vb. intrusion prevention system om inkomend en uitgaand dataverkeer te beoordelen op vooraf ingestelde regels)
Zie framedocument '07 Procedure-Gegevensbescherming en meldplicht datalekken'

8. Rechten van betrokkenen

Communiceer alle rechten aan de betrokkenen, dit zijn:

- Recht op inzage (toegang) tot de aanwezige/verwerkte gegevens.
- Recht op rectificatie: een betrokkene heeft het recht om een verzoek tot rectificatie in te dienen. Dit moet zonder onredelijke vertraging gebeuren.
- Recht om 'vergeten te worden': een dergelijk verzoek moet worden ingewilligd als één van de volgende gevallen van toepassing is:
  - De gegevens zijn niet langer nodig in verband met de doelen waarvoor zij zijn verzameld.
  - De betrokkene trekt de gegeven toestemming in, en er is geen andere rechtsgrond voor de verwerking.
  - De betrokkene maakt bezwaar tegen de verwerking.
  - De gegevens zijn onrechtmatig verwerkt.
  - De gegevens moeten worden gewist om te voldoen aan een wettelijke verplichting krachtig Unierecht of nationaal recht.
  - De gegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in art. 8 lid 1.
  - De voor verwerkingsverantwoordelijke moet redelijke maatregelen nemen om de gegevens te verwijderen, maar ook om iedere koppeling naar, kopie of reproductie te wissen.
- Recht op beperking van de verwerking.
- Recht op kennisgeving over de verwerking (en bij wijzigingen van persoonsgegevens): waaronder doel, categorieën van persoonsgegevens, ontvangers aan wie de gegevens worden verstrekt en opslagperiode.
- Recht op overdraagbaarheid van gegevens ('data-portability'): bij aanvraag van een persoon, in een gangbaar bestandsformaat, denk aan bijv. klanten, huisarts, energieleverancier.
- Recht op stellen van vragen, indienen klacht of bezwaar.
- Recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit.

***Borgen van de rechten: intern* privacybeleid, onderdeel arbeidsovereenkomst of huishoudelijk reglement via de inwerkchecklist; extern privacystatement / verklaring, algemene voorwaarden, cookiebeleid.**
Denk aan de AVG, Cookiewet en de Telecommunicatiewet.
Stel bij iedere verwerking van persoonsgegevens de vraag: hoe weet een persoon dat zijn/haar gegevens worden verwerkt en op welke wijze dit gebeurt?

Heldere informatie: informeer de betrokkenen over:

- Naam en contactgegevens verantwoordelijke
- Het doel en de rechtsgrond van de verwerking
- Informatie over eventuele geautomatiseerde besluitvorming
- (Categorieën van) ontvangers van de persoonsgegevens
- Indien van toepassing: passende waarborging die zijn genomen als de gegevens buiten de EU / EER worden doorgegeven
- De bewaartermijn of de criteria hiervan
- De rechten van betrokkene
- Informatie over de mogelijkheid een klacht in te dienen bij bedrijf of AP

9. Context-aansluiting

Als je als organisatie in meerdere landen gevestigd bent, dan mag je je leidende toezichthouder bepalen. Hoofdregel is dat het land waar de hoofdvestiging staat, de leidende toezichthouder wordt, bijvoorbeeld Nederland met de AP.

Dit stappenplan is een compliance aan de AVG. Denk ook aan andere geldende wetgeving in uw sector, zoals de Wet geneeskundige behandelingsovereenkomst, Archiefwet 1995 of regelgeving bij politie- en opsporingsdiensten, medische sector, media of telecom.

10. Periodiek actueel houden

Je moet ervoor zorgen dat persoonsgegevens correct zijn en blijven. Ook dienen deze gegevens niet langer bewaard te worden dan nodig is voor het doel waarvoor ze verzameld zijn. Neem dit bijvoorbeeld op in een MT-overleg of jaarevaluatie. Vraag met enige regelmaat af: geldt de huidige toestemming van betrokkenen nog, kunnen betrokkenen dit net zo gemakkelijk weer intrekken. Moeten er oude persoonsgegevens opgeruimd worden? Is je gegevenswerverwerking en risicomanagement up-to-date.

Meer informatie:

- https://autoriteitpersoonsgegevens.nl
- https://www.privacy-advocaat.nl/downloads