**Vragenlijst AVG 2018**

1. Hoe ziet uw organisatie er uit?
Maak een onderscheid tussen dochtermaatschappijen en moedermaatschappij in Nederland of elders in de EER (EU en Noorwegen, Liechtenstein en Andorra).
2. Voor welke organisatie of vestiging(en) vult u deze vragenlijst in?
3. In welke branche ben u werkzaam?
4. Wie zijn uw klanten?
In welke branche zijn uw bedrijfsmatige klanten vooral werkzaam?
5. Is het gebruikelijk dat er een jaarlijkse audit plaatsvindt? Zo ja, welke? ( denk aan ISO en Nen normering)
6. Welke persoonsgegevens worden er bij u verwerkt? (Denk hierbij aan het opslaan, analyseren, verstrekken, anonimiseren.. etc. van de persoonsgegevens)
7. Waarom worden deze persoonsgegevens verwerkt? (doeleinden)
8. Zijn al deze persoonsgegevens hiervoor noodzakelijk ? (dataminimalisatie)
9. Wat gebeurt er met deze persoonsgegevens?
10. Van wie zijn deze persoonsgegevens?
11. Vraagt u toestemming van de betrokkenen voor het verwerken van de persoonsgegevens? Zo ja, hoe wordt deze toestemming door de betrokkenen gegeven?
12. Kunt u de gegevens verwijderen of wijzigen als de betrokkene hierom vraagt?
13. Geeft u de betrokkenen een mogelijkheid deze toestemming naderhand in te trekken?
14. Op welke wijze geschiedt verstrekking van persoonsgegevens aan u? Via een formulier, digitaal of anders bijv. via een doorverwijzing?
15. Zijn de gegevens die aan u worden verzonden, versleuteld verzonden?
16. Bewaart u de gegevens op een server bij uw ict-leverancier? Of elders? Indien elders, waar vindt in de EER de opslag van deze gegevens plaats?
17. Is er een waarschijnlijkheid dat uw gegevensverwerking een hoog privacy risico oplevert voor de betrokkenen? (Denk hierbij bijvoorbeeld aan het evalueren van persoonlijke aspecten, het op grote schaal bijzondere persoonsgegevens verwerken of mensen volgen in een publiek toegankelijk gebied.)
18. Welke waarborgen treft u omtrent het verwerken en opslaan van de persoonsgegevens?
19. Heeft u een beleid betreffende het omgaan met persoonsgegevens en met datalekken?
20. Documenteert u alle informatie betreffende datalekken? (Denk hierbij bijvoorbeeld aan tijd, aard en maatregelen die genomen worden.)
21. Zijn alle gegevens van de betrokkenen makkelijk voor u te achterhalen dan wel te verzamelen?
22. Op welke wijze vindt opslag en registratie van persoonsgegevens van uw personeel plaats?

1. Hoeveel personeel heeft u in dienst?

1. Welke werknemers hebben er toegang tot de persoonsgegevens?
2. Is het noodzakelijk dat de werknemers voor de uitoefening van hun functie toegang hebben tot de persoonsgegevens? Is het noodzakelijk dat de personen toegang hebben tot *alle* gegevens?
3. Zijn uw werknemers zich ervan bewust hoe om te gaan met persoonsgegevens? Bespreekt u dit onderdeel bij indiensttreding met hun en schenkt u daar periodiek aandacht aan?
4. Maakt een specifiek geheimhoudingsbeding dan wel een ander beding ten aanzien van het omgaan met persoonsgegevens onderdeel uit van de arbeidsovereenkomst of van het personeelsreglement c.q. de huisregels?
5. Zorgt u ervoor dat bij een arbeidsconflict of bij uitdiensttreding werknemers direct geblokkeerd worden van de toegang tot de persoonsgegevens?
6. Heeft u een Functionaris Gegevensbescherming aangesteld of dit extern uitbesteed?
7. Maakt u gebruik van specifieke voor uw branche geschreven software? Zo ja, welke?

1. Geldt er specifieke wetgeving voor uw organisatie? Zo ja, welke?
2. Maakt u gebruik van een adequate firewall en virusscanner? Zijn deze up to date?
3. Maakt u periodiek een back up van de gegevens en zo ja, waar en hoe wordt de back up opgeslagen?
4. Welke derden hebben toegang tot uw kantoor?
5. Hebben deze derden ook toegang tot uw persoonsgegevens?
6. Aan welke derden verstrekt u persoonsgegevens om diensten voor u uit te voeren?

1. Heeft u overeenkomsten met derden waarin al rekening wordt gehouden met de bescherming van persoonsgegevens?

1. Weten de betrokkenen met welke derden u de gegevens deelt?
2. Controleert u deze derden die uw gegevens verwerken op de uitvoering van beveiligingsmaatregelen en regels rondom datalekken?

1. Heeft u een overzicht van al uw inkomende en uitgaande gegevensstromen?
2. Heeft u een overzicht van uw verdere gegevensverwerking? Zo ja, welke informatie documenteert u?
3. Heeft u inzicht in eventuele specifieke bewaartermijnen, die voor uw organisatie c.q. voor de persoonsgegevens die u verzamelt, gelden?
4. Heeft u vastgesteld hoe lang u verschillende categorieën gegevens bewaart? (bewaartermijnen)
5. Maakt u gebruik van een privacyverklaring op uw website?

1. Geeft u betrokkenen de mogelijkheid hun persoonsgegevens in te zien, te rectificeren, te wissen of over te dragen?

1. Heeft u in uw kantoorpand en uw terrein camerabewaking? Zo ja, heeft u een camerareglement?
2. Heeft u een ondernemingsraad of een PVT (personeelsvertegenwoordiging)?
3. Heeft u specifieke verzoeken met betrekking tot deze audit?
4. Wilt u bijlagen van relevante documenten bijvoegen?

Zoals:

* Arbeidsovereenkomst
* Verwerkersovereenkomst
* Personeelsreglement
* Overeenkomst van opdracht
* Huisregels/ Personeelshandboek
* Behandelovereenkomst
* Algemene voorwaarden
* Overeenkomsten met derden
* Anders, namelijk: