**Vragenlijst AVG 2018**

|  |
| --- |
| 1. Hoe ziet uw organisatie eruit? Maak een onderscheid tussen dochtermaatschappijen en moedermaatschappij in Nederland of elders in en/of buiten de EU. (Nb. voeg indien aanwezig een organogram toe) |
| 1. In welke branche is uw organisatie actief? |
| 1. In welke branche zijn de klanten van uw organisatie actief? |
| 1. Is het gebruikelijk dat er een jaarlijkse audit plaatsvindt? Zo ja, welke? (denk aan ISO en NEN normering) |
| 1. Welke persoonsgegevens[[1]](#footnote-1) worden er bij uw organisatie verwerkt? (Denk hierbij aan het opslaan, analyseren, verstrekken, anonimiseren enz. van persoonsgegevens) . Stel bij voorkeur een lijst op. |
| 1. Waarom worden deze persoonsgegevens verwerkt? (doeleinden) |
| 1. Wat gebeurt er met deze persoonsgegevens? |
| 1. Van wie zijn deze persoonsgegevens? (klanten, personeel, derden) |
| 1. Vraagt uw organisatie altijd toestemming van de betrokkenen voor het verwerken van de persoonsgegevens? Zo ja, hoe wordt deze toestemming door de betrokkenen gegeven? |
| 1. Geeft uw organisatie betrokkenen een mogelijkheid deze toestemming naderhand in te trekken? |
| 1. Op welke wijze geschiedt verstrekking van persoonsgegevens aan uw organisatie? Via een formulier, digitaal of anders bijv. via een doorverwijzing? |
| 1. Zijn de gegevens die aan uw organisatie worden verzonden, versleuteld verzonden? En de gegevens die u zelf verstuurd naar derden? |
| 1. Bewaart uw organisatie de gegevens op een server bij haar ICT-leverancier op een eigen server of of elders? Indien elders, waar vindt de opslag van deze gegevens plaats? |
| 1. Is er een waarschijnlijkheid dat de gegevensverwerking door uw organisatie 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 het volgen van mensen in een publiek toegankelijk gebied, bijvoorbeeld met camera’s). |
| 1. Welke waarborgen treft uw organisatie omtrent het verwerken en opslaan van de persoonsgegevens? |
| 1. Heeft uw organisatie een beleid betreffende het omgaan met persoonsgegevens en met datalekken? |
| 1. Documenteert uw organisatie alle informatie betreffende datalekken? (Denk hierbij bijvoorbeeld aan tijd, aard en maatregelen die genomen worden). |
| 1. Zijn alle gegevens van de betrokkenen makkelijk te achterhalen dan wel te verzamelen? |
| 1. Op welke wijze vindt opslag en registratie van persoonsgegevens van het personeel van uw organisatie plaats? |
| 1. Hoeveel personeel heeft uw organisatie in dienst? |
| 1. Welke werknemers hebben er toegang tot de persoonsgegevens? |
| 1. 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? |
| 1. Zijn de werknemers van uw organisatie zich ervan bewust hoe om te gaan met persoonsgegevens? Bespreekt uw organisatie dit onderdeel bij indiensttreding met hun en wordt daar periodiek aandacht aan besteed? |
| 1. 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? |
| 1. Zorgt uw organisatie ervoor dat bij een arbeidsconflict of bij uitdiensttreding werknemers direct geblokkeerd worden van de toegang tot de persoonsgegevens? |
| 1. Maakt uw organisatie gebruik van specifieke voor de branche geschreven software? Zo ja, welke? |
| 1. Geldt er specifieke wetgeving voor uw organisatie? Zo ja, welke? |
| 1. Maakt uw organisatie gebruik van een adequate firewall en virusscanner? Zijn deze up to date? |
| 1. Maakt uw organisatie periodiek een back up van de gegevens en zo ja, waar en hoe wordt de back up opgeslagen? |
| 1. Welke derden hebben toegang tot de kantoren? |
| 1. Hebben deze derden ook toegang tot de persoonsgegevens van uw organisatie? |
| 1. Aan welke derden verstrekt uw organisatie persoonsgegevens om diensten voor haar uit te voeren? |
| 1. Heeft uw organisatie overeenkomsten met derden waarin al rekening wordt gehouden met de bescherming van persoonsgegevens? |
| 1. Heeft uw organisatie een overzicht van al haar inkomende en uitgaande gegevensstromen? |
| 1. Heeft uw organisatie een overzicht van haar verdere gegevensverwerking? Zo ja, welke informatie documenteert uw organisatie? |
| 1. Heeft uw organisatie inzicht in eventuele specifieke bewaartermijnen, welke gelden voor haar organisatie c.q. voor de persoonsgegevens die uw organisatie verzamelt,? |
| 1. Maakt uw organisatie gebruik van een privacyverklaring op de website? |
| 1. Geeft uw organisatie betrokkenen de mogelijkheid hun persoonsgegevens in te zien, te rectificeren, te wissen of over te dragen? |
| 1. Heeft uw organisatie in haar bedrijfsruimte en op haar terrein camerabewaking? Zo ja, heeft uw organisatie een camerareglement? |
| 1. Heeft uw organisatie een ondernemingsraad of een personeelsvertegenwoordiging? |

Beschikt uw organisatie over een of meer van de navolgende documenten? Zo ja, graag een kopie hiervan bijsluiten:

* Arbeidsovereenkomst
* Personeelsreglement/huisregels
* Overeenkomst met derden die in opdracht van uw organisatie persoonsgegevens verwerken (ICT-bedrijf, accountant, loonadministratie, vervoersbedrijvenenz.)
* Be- of verwerkersovereenkomsten
* Algemene Voorwaarden
* Privacyverklaring website
* Anders, namelijk……………

1. Elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon; elk gegeven dat herleidbaar is tot een individu. [↑](#footnote-ref-1)