BIJLAGE 3 Meer informatie

Hierna volgt enige context ten aanzien van AVG en informatiebeveiliging van gebruikte systemen.

Belangrijke factoren om rekening mee te houden bij verwerking van persoonsgegevens

Wanneer je met persoonsgegevens of bedrijfsgevoelige gegevens werkt, zijn er een aantal "triggers" waar je extra alert bij moet zijn. Want hoe je het ook regelt, jij blijft volgens de AVG verantwoordelijk voor het verwerken van persoonsgegevens.

- Verwerk je gegevens voor je eigen organisatie of voor een andere organisatie (bijvoorbeeld wanneer je een dienst levert)?
- Zijn de gegevens die je verwerkt op een of andere manier gevoelig (medisch, minderjarigen, financieel etc.)?
- Worden ze opgeslagen in Europa?
- De Autoriteit Persoonsgegevens en de AVG eisen dat je persoonsgegevens verantwoordelijk, veilig en binnen de kaders van de wet persoonsgegevens verwerkt. Maar ook bedrijfsgevoelige gegevens als jaarrekeningen en prognoses wil je niet per ongeluk verkeerd delen. Het is belangrijk om je keuzes regelmatig te controleren en een plan te maken voor het oplossen van eventuele problemen om te blijven voldoen aan je eigen eisen en die van de AVG. Dat toont ook aan dat je professioneel met gegevens omgaat. Wanneer je als instelling subsidie ontvangt, maakt dit ook onderdeel uit van je risicobeheersing, waarover je jaarlijks in het bestuursverslag verantwoording aflegt.

Waar moet je op letten in algemene voorwaarden of verwerkingsovereenkomst?

Er zijn (juridische) experts die je kunnen helpen. Bij twijfel kun je de hulp van deze personen inschakelen. Daarnaast zijn er ook zaken waar je zelf al rekening mee kunt houden.

Wettelijk moet je een aantal zaken regelen:

- Het eigendom van gegevens

- Doorgifte en gebruik van gegevens
- Geheimhouding van gegevens
- (Informatie)veiligheid van gegevens

Hierover maak je afspraken. Vaak doe je dat als onderdeel van algemene voorwaarden bij grotere leveranciers als Google en Microsoft. Dan heb je zelf niet altijd voldoende opties om aan de AVG te blijven voldoen. Werk daarom als het even kan met een aparte geheimhoudingsovereenkomst en verwerkingsovereenkomst. Daarnaast kun je met sommige bedrijven in de leveringsvoorwaarden en met specifieke overeenkomsten ook van alles regelen. In dat geval is het zeker raadzaam om een (juridisch) expert in te schakelen.

Het is daarnaast ook raadzaam om regelmatig (bijvoorbeeld jaarlijks) te checken of er wijzigingen zijn in de voorwaarden van je leveranciers. Dit is voor gesubsidieerde instellingen ook onderdeel van je aanpak ten aanzien van je risicobeheersing.

We adviseren om de volgende passages in overeenkomsten extra zorgvuldig te lezen.

- AANSPRAKELIJKHEID - de AVG stelt dat zowel jouw instelling als de leverancier aansprakelijk zijn naar de betrokkene. Je kunt dus niet de volledige verantwoordelijkheid bij je leverancier neerleggen. Omgekeerd kan de leverancier dat ook niet volledig bij jou neerleggen.
- SOORT GEGEVENS - stel vast dat de gegevens die de leverancier zegt te verwerken, overeenkomen met wat je hebt afgesproken.
- VERWERKING OP EUROPEES GRONDGEBIED of volgens de in Europa geldende standaarden - Dit is een actueel punt: zorg ervoor dat je leverancier de persoonsgegevens in Europa verwerkt of zich aan goedgekeurde afspraken houdt. LET OP: *in de zomer van 2020 is een uitspraak van het Europees Hof gedaan, waarin werd gesteld dat de EU-VS Privacy Shield herzien moet worden. De EU-VS Privacy Shield is een overeenkomst over de bescherming van persoonsgegevens van burgers van de Europese Unie, die in de Verenigde Staten worden verwerkt. Voor Amerikaanse leveranciers als Google, Zoom en Microsoft kan deze veranderende wetgeving dus ineens heel actueel worden.*
- EIGEN VERWERKINGSOVEREENKOMST OF ONDERDEEL ALGEMENE VOORWAARDEN - je bent wettelijk verplicht om hier afspraken over te maken. Als er geen aparte verwerkingsovereenkomst is, dienen er minimale artikelen in de algemene voorwaarden te staan.

- **Geheimhouding** – het is altijd goed om te controleren of de voorwaarden stellen dat je leverancier alleen gegevens verwerkt voor het doel waarvoor ze worden verstrekt en er geen doorgifte aan derden plaatsvindt.
- **Beveiliging** – dit is geheel afhankelijk van je eigen kennis en het soort gegevens dat de leverancier verwerkt, maar je prikt er snel doorheen als een organisatie hier niet over nagedacht heeft. Een ISO- of NEN-norm is altijd een snelle check. Hoewel het niet hebben van een ISO- of NEN-certificaat niet automatisch betekent dat gegevens onveilig verwerkt worden.