Beleid Informatiebeveiliging en privacy

1. Inleiding
Hieronder een korte samenvatting van de uitgangspunten waar Orionis Walcheren informatiebeveiliging en privacy heeft gebaseerd.

Orionis Walcheren gaat er van uit dat de opdrachtnemer bekend is met de normen voor informatiebeveiliging, ISO 27001, de Baseline Informatiebeveiliging Overheid (BIO) en de normen voor privacy, de Algemene Verordening Gegevensbescherming (AVG).

2. Informatiebeveiliging, de Baseline Informatiebeveiliging Overheid
Orionis Walcheren volgt de Baseline Informatiebeveiliging Overheid (BIO) zie link naar informatie over de Baseline informatiebeveiliging Overheid. De BIO is verwerkt in verschillende strategische beleidsplannen en tactisch beveiligingsplannen.

3. Privacy, de Algemene verordening gegevensbescherming (AVG)
Als er sprake is van verwerken van persoonsgegevens, dan moet worden voldaan aan de AVG. Een persoonsgegeven omvat 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon'.
Verwerken moet ruim worden geïnterpreteerd. Onder verwerken wordt verstaan 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens'.

3.1 Wettelijke grondslag
Het mogen verwerken van persoonsgegevens mag alleen als er hiervoor een wettelijke grondslag en een rechtvaardig doel (doelbinding) is. Het verwerken van persoonsgegevens in een zaaksysteem is voor Orionis Walcheren gebaseerd op een geldige wettelijk grondslag uit de AVG met een gerechtvaardigd doel. Verwerking is toegestaan maar dan nog moet deze verwerking aan eisen voldoen.

3.2 Passende technische en organisatorische maatregelen
Op grond van artikel 32 AVG moeten er passende technische en organisatorische maatregelen getroffen worden om een op het risico afgestemd beveiligingsniveau te waarborgen.
Waarborgen kunnen o.a. zijn:
- het kunnen pseudonimiseren en versleutelen van persoonsgegevens;
- het vermogen om bij een technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen. Denk hierbij aan een goed back-up systeem;
- het hebben van een goed continuïteitsmanagement;
- het hebben van een goed toegangsbeleid. Denk hierbij aan multifactor authenticatie;

- het treffen van maatregelen om ervoor te zorgen dat alleen bevoegde personen toegang hebben tot de persoonsgegevens. Denk hierbij aan een goed autorisatiemodel en het loggen van verwerkingen in de applicatie;
- het hebben van goede bewaar- en vernietigingsmogelijkheden;
- het ISO 27001 gecertificeerd zijn.

3.3 Privacy bij design

De technische maatregelen kunnen worden toegepast door het principe privacy bij design. In dit geval beter, "Archiveren by Design". Dit is de basis om te kunnen voldoen aan wetgeving en kaders op het gebied van informatiebeheer. Het inbedden van recordmanagement bij het inrichten van een zaaksysteem zorgt voor een goede toegankelijkheid, de naleving van de bewaartermijnen en de het kunnen delen van informatie.

3.4 Privacy by default

Artikel 25 AVG verplicht in artikel 25 tot het nemen van maatregelen om persoonsgegevens te beschermen bij ontwerp en standaardinstellingen van informatiesystemen. Dit betekent beperking van de toegang tot informatie en systemen met persoonsgegevens. Dit kan via autorisaties en andere vormen van toegangsbeheer tot alleen bevoegde personen die voldoen aan het principe 'need to know'. Kortom, dus beperking van de toegang door toegangsautorisaties, logging en monitoring.

3.5 Rechten van betrokkenen

Gewaarborgd moet zijn dat betrokkenen in staat zijn 'in control' te zijn over hun eigen persoonsgegevens. Ze hebben het recht om te weten wat er met hun persoonsgegevens gebeurt en indien nodig hierop invloed uit te oefenen. Belangrijk is dat betrokkenen:

- inzage kan hebben in zijn/haar persoonsgegevens (art. 15 AVG)
- rectificatie van persoonsgegevens kan eisen (art. 16 AVG)
- persoonsgegevens kan laten wissen(art. 17 AVG)
- beperking van verwerking kan eisen (dataminimalisatie, art. 18 AVG)
- persoonsgegevens kan meenemen (dataportabiliteit art. 20 AVG)
- bezwaar kan maken tegen de verwerking (artikel 21 AVG);

Bovenstaande is niet helemaal volledig maar daar waar dingen ontbreken, kan gesteld worden dat de AVG nageleefd moet worden.