



## Managementsamenvatting

Vanaf 2018 heeft de StOET een Functionaris voor de Gegevensbescherming aangesteld, waarmee een praktische invulling van het (per 25-5-2018 verplicht) toezicht op naleving van de Algemene Verordening Gegevensbescherming is gegeven. Sinds januari 2021 is binnen de StOET de Functionaris voor de Gegevensbescherming (FG) aangesteld vanuit Privacy1.

Naast de specifieke expertise die een interne toezichthouder heeft, kan door het aanstellen van een FG een terughoudende opstelling van de Autoriteit Persoonsgegevens (hierna: AP) worden verwacht.

De FG is een deskundig aanspreekpunt voor de StOET voor wat betreft de AVG. Ook kan de FG als contactpersoon optreden voor betrokkenen (bij eventuele vragen en klachten). Daarnaast vergroot een FG het privacybewustzijn binnen de StOET. Tegelijkertijd kan worden gewerkt aan een effectieve en eigentijdse invulling van AVG. De FG is onafhankelijk, art. 21 WOR is van toepassing op de FG. De adviezen zijn niet bindend, de verwerkingsverantwoordelijke heeft de vrijheid afwijkende beslissingen te nemen.

In dit document wordt enerzijds teruggekeken naar de resultaten zoals die zijn geboekt in 2022 en inzicht verschaft in de geplande activiteiten in 2023.

## Introductie

De Algemene Verordening Gegevensbescherming heeft tot gevolg dat regels aangaande de bescherming van persoonsgegevens aangescherpt zijn. Ook de StOET zal transparant moeten zijn (en blijven) in hun beleid en omgang met persoonsgegevens, maar ook aan kunnen tonen dat zij een passende implementatie hebben en controlemaatregelen hebben getroffen. Zo is voor de StOET de inzet van een FG verplicht met name daar waar de verwerking van bijzondere persoonsgegevens tot de primaire taak behoort. Zelfregulering en integratie van het toezicht in de normale bedrijfsvoering leveren een effectieve bijdrage aan het realiseren van *privacy governance/ compliancy*. Het toezicht leidt er -als onderdeel van het kwaliteitsbeleid van de StOET- toe dat patiënten en medewerkers vertrouwen kunnen hebben en houden in de wijze waarop de StOET met hun persoonsgegevens omgaat.

Op basis van zowel de AVG en de algemeen aanvaarde standaard(en) voor informatiebeveiliging zal de FG een stelsel van maatregelen ter bescherming van privacy en waarborging van vertrouwelijkheid, integriteit en beschikbaarheid van informatie(voorziening) binnen de StOET entameren en daarop toezien.

De FG heeft 3 raakvlakken, te weten:

1. de betrokkene over wie gegevens worden verwerkt,
2. de organisatie die verantwoordelijke is van de verwerkingen en
3. De AP, waarbij hij als intermediair optreedt.

## Resultaatsgebieden FG

In dit onderdeel wordt per resultaatsgebied aangegeven welke activiteiten in 2022 zijn uitgevoerd en welke activiteiten aandacht krijgen in 2023.

### *Controle en registratie*

- Het toezicht houden op de implementatie en naleving van het (interne) privacybeleid en het informatiebeveiligingsbeleid.

### ***Privacybeleid (verantwoordingsdocument)***

In 2022 is door de StOET het verantwoordingsdocument vastgesteld. Het document beschrijft de mate van 'privacy compliance' en geeft implementatievoorstellen weer. Deze voorstellen zijn voor dit rapport als uitgangspunt genomen, naast de plannen uit het jaarverslag van 2021/2022. Aangezien de StOET een kleine organisatie is, kan het verantwoordingsdocument als privacybeleid worden beschouwd.

### *Opstellen beleid*

In het jaarrapport van 2021/2022 stond aangegeven dat in 2022 aan de hand van het verantwoordingsdocument werkinstructies en procedures zouden worden opgesteld. Ook zouden in 2022 medewerkers worden getraind en een overleg hebben plaatsgevonden met de Research Commissie. Deze activiteiten worden doorgeschoven naar 2023.

In 2022 zijn in ieder geval de volgende instrumenten opgesteld:

- register van verwerkingen;
- privacyverklaring;
- standaard (sub-)verwerkerovereenkomst;
- procedure melden datalekken;
- template DTA.

### *Privacy implementatie in 2023*

De FG/ kwaliteitsfunctionaris zullen doorgaan met:

- het uitvoeren of initiëren van dataprotectie impact assessments-, risicoanalyses en interne audits;
- het opstellen van werkinstructies en trainen van medewerkers en de leden van de Research Commissie;
- het verhogen van het medewerkersbewustzijn rondom beveiligingsincidenten, datalekken en overige risico's (incl. het verhogen van de digitale weerbaarheid);
- het opzetten of initiëren van een registratie voor privacy-inbreuken en beveiligingsincidenten, alsmede het afhandelen van opgetreden incidenten en het nemen van preventieve maatregelen ter voorkoming van dergelijke incidenten.

*De FG heeft de verwerkingsverantwoordelijke bijgestaan bij het al dan niet melden van datalekken.*

*In 2022 werden geen incidenten geregistreerd.*

### *Communicatie en voorlichting*

- Het onderhouden van externe en interne contacten op alle niveaus binnen dit kader.

*De FG en de kwaliteitsfunctionaris hebben iedere twee maanden een online overleg waar actuele zaken en doorlooptijden van acties worden besproken. Binnen de StOET is de FG goed zichtbaar, vindbaar en benaderbaar voor vragen en advies. In 2023 zal de FG de zichtbaarheid verder vergroten o.a. door medewerkers te trainen en een sessie te organiseren met de leden van de Research Commissie.*

- Het organiseren van en deelnemen aan coördinerende overleggen met betrekking tot privacybescherming en informatiebeveiliging.
- Het verzorgen en coördineren van voorlichting en interne opleidingen van het personeel op het gebied van informatiebeveiliging en privacybescherming.
- Het stimuleren van het privacy- en beveiligingsbewustzijn en het opstellen, uitvoeren en onderhouden van een communicatieplan.
- Het volgen van nieuwe ontwikkelingen en wet- en regelgeving op het gebied van informatiebeveiliging en privacybescherming.

*De FG en Kwaliteitsfunctionaris houden de ontwikkelingen inzake de AVG nauwlettend bij. De FG is als expert verbonden aan de ELSI-servicedesk en lid van Coreon (Federa).*

### *Advies en rapportage*

- Het optreden als projectmanager bij beveiligingsprojecten, waarbij aansturing wordt gegeven aan projectleiders binnen organisatorische eenheden.
- Het afstemmen van privacybescherming en informatiebeveiliging met lopende projecten binnen de organisatie.

*In 2022 zijn verschillende adviezen verstrekt:*

- verwerkersovereenkomst met ICT-leveranciers;*
- koppelingen met externe registraties (waaronder IKNL en PALGA), maar ook de BRP;*

*-Overeenkomst met onderzoekers (DTA) aan de hand van het NFU-template;  
-geldigheidsduur Informed consent;  
-voorbeeldbrief voor artsen over toestemming;  
-vraag over backup van gegevens;  
-teksten op de website;  
-vragen van collega FG's van zorginstellingen (waaronder het Haga).*

- Het uitwerken van privacybeschermings- en informatiebeveiligingsplannen ten aanzien van de maatregelen, alsmede het leveren van ondersteuning bij het uitvoeren van de geaccepteerde plannen.
- Het geven van gevraagd en ongevraagd advies aan de leiding van de organisatie en het lijnmanagement over de te nemen maatregelen.
- Het rapporteren aan de leiding van de organisatie over het gevoerde beleid met betrekking tot privacybescherming en informatiebeveiliging, de voortgang van implementatie van nieuwe maatregelen, opgetreden incidenten, ondernomen acties, resultaten van onderzoeken en resultaten van controles.

### **Conclusies en aanbevelingen**

In 2023 zal de focus van de FG meer gelegd worden op het opstellen en trainen van medewerkers inzake werkinstructies en procedures. Daarnaast zal worden gewerkt aan een samenwerkingsovereenkomst met PALGA. Naast de AVG-onderwerpen zullen medewerkers ook meer te maken krijgen met dreigingen op het gebied van cybersecurity. Hier zal in de training eveneens aandacht aan worden besteed, eveneens aan het herkennen en melden van datalekken. Ook daar zal in 2023 aandacht voor zijn. Ook zal in 2023 een DPIA op de verwerking van bijzondere persoonsgegevens worden uitgevoerd (dit is in 2022 niet gedaan). Met deze stappen groeit de StOET verder in privacy-volwassenheid en kan de StOET aantoonbaar voldoen aan de vereisten van de AVG.