Titel:	**Jaarverslag 2020/2021 en jaarplan 2022** **Functionaris voor Gegevensbescherming**
Opdracht:	StOET
Reikwijdte:	Kwaliteitsfunctionaris en directeur StOET
Eigenaar / Auteur:	Marie-José Bonthuis – Privacy1
Datum:	3-1-2022
Doel: Inzicht verschaffen in activiteiten en plannen van de Functionaris voor Gegevensbescherming (FG).	

Managementsamenvatting

Per januari 2021 is binnen de StOET een Functionaris voor de Gegevensbescherming (FG) vervangen. Hiermee blijft een praktische invulling van het (per 25-5-2018 verplicht) toezicht op naleving van de Algemene Verordening Gegevensbescherming gegeven.
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 verantwoordelijke heeft de vrijheid afwijkende beslissingen te nemen.

In dit document wordt teruggekeken naar de resultaten zoals die zijn geboekt in 2021 en inzicht verschaft in de geplande activiteiten in 2022.

Introductie

De Algemene Verordening Gegevensbescherming heeft tot gevolg gehad 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 2021 zijn uitgevoerd en welke activiteiten aandacht krijgen in 2022.

Controle en registratie

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

> ***Privacybeleid (verantwoordingsdocument)***
> De FG heeft in 2021 een concept verantwoordingsdocument opgesteld, naar aanleiding van een inventarisatie en documentenscan (mappen). De kwaliteitsfunctionaris van de StOET heeft een personeelshandboek opgesteld, waar ook het omgaan met persoonsgegevens en *devices* in is beschreven.

Opstellen beleid

Het verantwoordingsdocument, dat dient als intern privacybeleid, zal in Q1 2022 kunnen worden vastgesteld. Aan de hand daarvan zullen werkinstructies en procedures worden opgesteld.

Ook zullen in 2022 medewerkers worden getraind. In 2022 zal dan ook een organisatiebreed privacybeleid inclusief het implementeren en onderhouden van instrumenten zijn opgesteld zijn met een verwijzing naar:
-register van verwerkingen;
-privacyverklaring;
-(sub-)verwerkerovereenkomst;
-procedure melden datalekken.

Privacy implementatie in 2022
Met een uniforme en periodieke assessment (m.b.v. het Privacy Volwassenheidsmodel in het verantwoordingsdocument) kan de FG de status van de privacy initiatieven in kaart brengen. De uitkomsten kunnen worden gebruikt als analyse en evaluatie-instrument voor (hoger) management.

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;
  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 verantwoordelijke bijgestaan bij het al dan niet melden van datalekken.

In 2021 werden geen incidenten geregistreerd.

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

De FG is in 2021 ingeschreven in het register van het AP en vermeld op de website, zij is daarmee voor het publiek een zichtbare figuur. Binnen de StOET is de FG goed zichtbaar, vindbaar en benaderbaar voor vragen en advies. In 2022 zal de FG de zichtbaarheid vergroten o.a. door medewerkers te trainen.

- 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 2021 zijn verschillende adviezen verstrekt:
-verwerkersovereenkomst met ICT-leveranciers;
-koppelingen met externe registraties (waaronder PALGA);
-Overeenkomst met onderzoekers (DMTA);
-geldigheidsduur informed consent;

- 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.

Onder leiding van de FG zijn in 2021 een aantal medewerkers opgeleid op het gebied van de AVG en anonimisering van gegevens.

Conclusies en aanbevelingen
In 2022 kan de focus van de FG meer gelegd worden op het onderhouden van de bestaande instrumenten, waaronder het register van verwerkingen, de verwerkersovereenkomsten etc.
Ook zal o.b.v. het verantwoordingsdocument (dat in 2022 zal worden vastgesteld) werkinstructies en procedures worden opgesteld en worden geïmplementeerd. Naast de AVG-onderwerpen zullen medewerkers ook meer te maken krijgen met dreigingen op het gebied van cybersecurity. Ook daar zal in 2022 aandacht voor zijn. Ook zal in 2022 een DPIA op de verwerking van bijzondere persoonsgegevens worden uitgevoerd. Met deze stappen groeit de StOET in privacy-volwassenheid en kan de StOET aantoonbaar voldoen aan de vereisten van de AVG.