

FG-gesprekskaart | AI & algoritmen

Bestuurlijke verantwoording

- Wat is de visie van het bestuur op digitalisering en de inzet van AI en algoritmen bij de verwerking van persoonsgegevens?
- Welke rol ziet het bestuur voor zichzelf rondom AI en algoritmen?
- Is de toepassing van AI of algoritmen goed uitlegbaar aan de medewerkers en studenten of deelnemers van een onderzoek? Op welke manier/in welke vorm gebeurt dit?
- Op welke manier krijgt het bestuur informatie over risico's van AI en algoritmen binnen de organisatie?
- Door wie vindt de besluitvorming plaats om AI en algoritmen in te zetten?

Ethiek

- Hoe worden ethische vraagstukken beoordeeld en op welke manier wordt dit geïntegreerd in besluitvorming?
- Bestaan er formele werkwijzen (bijvoorbeeld een ethische commissies, richtlijnen, formats) om data-ethische vraagstukken bespreekbaar te maken? En functioneren deze ook?
- Hoe wordt omgegaan met mogelijke bias en discriminatie bij de inzet van AI en algoritmen?
- Is een FRIA/IAMA* verplicht voor het AI-systeem? Zo ja, wat waren de uitkomsten van deze beoordeling?

* FRIA - Fundamental Rights Impact Assessment. In de Nederlandse context voor de FRIA-verplichting uit artikel 27 van de AI-verordening is IAMA, Impact Assessment Mensenrechten en Algoritmen.

Naleving AVG

- Is de inzet van AI noodzakelijk en proportioneel voor het doel? Zijn er minder ingrijpende alternatieven overwogen?
- Wordt er voldaan aan transparantieplichtingen zoals informatieverstrekking aan betrokkenen over de verwerking?
- Op welke manier kunnen betrokkenen hun rechten uitoefenen?
- Is de verwerking van persoonsgegevens binnen het AI-systeem volledig inzichtelijk en onderbouwd? Zijn er bijzondere persoonsgegevens bij de verwerking betrokken?
- Is er een Data Protection Impact Assessment (DPIA) uitgevoerd door de privacyfunctionaris?
- Vinden er verdere verwerkingen plaats voor het trainen van AI-modellen, en zo ja, door wie en is dit goed onderbouwd?
- Is er sprake van geautomatiseerde besluitvorming of profilering? En zo ja, is er nagedacht over betekenisvolle menselijke tussenkomst? Hoe is dit uitgewerkt? Op wat voor soort fouten wordt gecheckt en werkt dit effectief?
- Is het transparant/begrijpelijk hoe het algoritme werkt?

Informatiebeveiliging

- Is er een toets uitgevoerd door informatiebeveiliging? Wat voor toets betreft dit? Wat waren de uitkomsten?
- Is er een BIV-score bekend en is er een risicoanalyse uitgevoerd?
- Hoe zijn technische en organisatorische maatregelen geborgd?
- Is de CISO betrokken bij de verwerking?

Inkoop/leveranciersbeheer

- Is het AI-systeem of algoritme zelf ontwikkeld of extern ingekocht?
- Zijn de AVG-rollen (verantwoordelijke, verwerker) voor de verwerking expliciet vastgesteld?
- Is er zicht op hoe de AVG-rollen zich verhouden tot rollen die staan beschreven in de AI-verordening?
- Is er (zo nodig) een verwerkersovereenkomst afgesloten met derden?
- Welke protocollen en afspraken gelden bij een datalek of incident?

Techniek

- Wat voor type AI of algoritme wordt toegepast (bijvoorbeeld deep-learning, machinelearning, regelgebaseerd algoritme)?
- Hoe wordt monitoring en evaluatie van (de effectiviteit van) het AI-systeem of algoritme geïmplementeerd?
- Hoe verloopt de datastroom van persoonsgegevens? Zijn de bronnen en verwerkingen in kaart gebracht?



Toelichting FG-gesprekskaart

De toezichthoudende rol van de Functionaris voor Gegevensbescherming (FG) op de verwerking van persoonsgegevens volgt uit de AVG. Dit toezicht gebeurt technologie-neutraal. Een verwerking van persoonsgegevens in een nieuw AI-systeem of algoritme valt binnen de reikwijdte van het toezicht.

De FG voert regelmatig het gesprek over AI-toepassingen. Deze FG-gesprekskaart helpt hierbij als inspiratiebron. De antwoorden dragen bij aan een beeld van hoe de organisatie omgaat met AI in relatie tot de verwerking van persoonsgegevens.

Rol van de FG (o.a.)

Advies | De FG adviseert bij het identificeren van mogelijke privacyrisico's rondom AI-toepassingen en het nemen van passende maatregelen om deze risico's te beheersen. Is er onduidelijkheid over de restrisico's dan kan de FG een voorafgaande raadpleging bij de AP adviseren.

Toezicht | De FG beoordeelt de privacyaspecten van AI-toepassingen. De FG controleert of de benodigde technische en organisatorische maatregelen zijn genomen om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens te borgen.

Samenwerking stakeholders | Om ervoor te zorgen dat privacy en gegevensbescherming adequaat worden aangepakt bij het gebruik van AI-technologieën, werkt de FG samen met andere relevante partijen, zoals de CPO, CISO, AI-officer en externe toezichthoudende autoriteiten.

Praktische tips

- Wees als FG alert op overlapping tussen AVG en de AI-verordening:
 - (bijzondere) persoonsgegevens
 - Profilering
 - geautomatiseerde (individuele) besluitvorming
 - beoordeling van de gevolgen voor grondrechten (DPIA, IAMA)
- Ga binnen de organisatie op bestuurlijk niveau het gesprek aan over wie toezicht houdt op AI en algoritmes.
- Communiceer binnen de organisatie waar de FG op let in het geval van AI en algoritmen.
- Besteed aandacht aan AI en algoritmen in het FG-jaarverslag in relatie tot de AVG en de bescherming van persoonsgegevens.
- De FG houdt ook bij AI en algoritmen toezicht op hoe de organisatie invulling geeft aan het treffen van passende technische en organisatorische maatregelen voor het juiste beveiligingsniveau met gebruik van moderne technieken. Houd daarbij rekening met de context, doelen van de verwerking en de uitvoeringskosten.

Scope

Deze gesprekskaart gaat over de toezichthoudende rol van de FG vanuit de AVG. De FG is niet de toezichthouder op de AI-verordening. De FG voert het gesprek over persoonsgegevens die in een AI-systeem worden verwerkt en adviseert wie hierover moet worden geconsulteerd om zo'n systeem veilig te gebruiken.