



**Centrale Ondernemingsraad**

**COR-secretariaat**

College van Bestuur van de Universiteit van Amsterdam  
Mw. prof. dr. G.T.M. ten Dam  
Spui 21  
1012 WX Amsterdam

Spui 21  
1012 WX Amsterdam  
Postbus 19268  
1000 GG Amsterdam

T 020 525 6955  
E-mail: cor@uva.nl

Datum  
21 juni 2018  
Contactpersoon  
E.B.I. Moors

Telefoon  
020 525 6955  
Bijlagen  
-

Uw kenmerk  
2018-023698/023700  
Ons kenmerk  
cor18/u020

Onderwerp

Instemmingsverzoek Privacybeleid en beleid verwerking persoonsgegevens; en instemmingsverzoek Reglement cameratoezicht

Geacht College,

De COR heeft uw memo d.d. 23 mei 2018 in goede orde ontvangen en waardeert de gevoerde dialoog en uitgebreide bespreking in de overlegvergadering van 18 mei en het technisch overleg van 4 juni 2018 over het Privacybeleid en beleid verwerking persoonsgegevens (hierna: Privacybeleid) en Reglement cameratoezicht (hierna: Camerareglement). Echter heeft de COR besloten om op beide stukken geen instemming te verlenen. Concreet gaat het om de volgende punten:

Ten aanzien van het Privacybeleid:

De COR stemt pas in met het Privacybeleid wanneer zijn instemmingsrecht voor inrichting en wijzigingen van het verwerkingsregister is erkend. Dit betreft procedures en instructies met betrekking tot personeelsgegevens, maar ook vaststelling van de verwerkingsdoeleinden, bewaartermijnen en toegangsautorisaties. Het Privacybeleid geeft de indruk dat deze doeleinden en andere bovengenoemde onderdelen in eerste instantie geformuleerd zullen worden in de verwerkingsregisters. Uit de Memorie van Toelichting bij de WOR leidt de COR af dat het instemmingsrecht met name van kracht is op de concrete uitwerking van de verwerkingen van personeelsgegevens, onder andere de vaststelling van de verwerkingsdoeleinden, de te verwerken (soorten) persoonsgegevens, de omgang daarmee en de begrenzing van deze verwerkingen.

Zorgpunt ten aanzien van de rol van de Functionaris Gegevensbescherming:

Het Privacybeleid bepaalt dat “de toegang” tot (de verwerking van) persoonsgegevens door autorisatietabellen wordt afgebakend. In de autorisatietabel wordt de volgende informatie opgenomen: naam of namen van de geautoriseerde(n) functionaris, functie, duur en omvang van de toegestane handelingen.” Wie de autorisatietabellen moet opstellen blijft in het midden, evenals de rechtmatigheidstoets die de Functionaris Gegevensbescherming (hierna: FG) zou moeten uitvoeren en de vereiste COR instemming voor opstelling en afbakening van toegang tot personeelsgegevens.

Nog voordat überhaupt van een verwerkingsregister sprake kan zijn, dienen volgens het Privacybeleid meldingen bij de FG ingediend te worden. Ook hier moet het Privacybeleid nog duidelijk maken wie dat dan moet doen en dat hier procedures/instructies voor volgen. Deze procedures moeten ook duidelijk maken dat de betreffende persoon wijzigingen in de verwerking van persoonsgegevens

Ons kenmerk  
cor18u/020

bijhoudt en meldt bij de FG, opdat deze de rechtmatigheid van de wijzigingen kan beoordelen, waar nodig de verwerkingsregisters aanpassen, waarna weer een instemmingsverzoek aan de COR volgt.

Ten aanzien van het Camerareglement:

In het Camerareglement ontbreken concrete procedures en instructies voor de personen die met het camerasysteem en de daarmee vastgelegde persoonsgegevens moeten werken. In het Camerareglement ziet de COR dat de FG positief advies moet geven voor het plaatsen van een camera alvorens tot plaatsing wordt overgegaan, als een noodzakelijke uitbreiding voordat de COR tot instemming overgaat. Immers onder artikel 27 lid 1 onder k en l van de WOR dient de ondernemer voorafgaande aan het invoeren van een regeling ten aanzien van het waarnemen van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen instemming te vragen aan de Ondernemingsraad. Dit geldt ook voor het plaatsen van heimelijke camera's.

In het overleg op maandag 4 juni heeft de bestuurder aangegeven de noodzakelijkheid van een positief advies van de FG ten aanzien van het cameratoezicht niet te kunnen inwilligen aangezien dat een inbreuk zou maken op de discretionaire bevoegdheid van het CvB. De inzet van een camera moet noodzakelijk zijn om de gestelde doeleinden te kunnen bereiken. Hierbij moeten de belangen van de betrokken werknemers worden meegewogen. Op deze belangen mag namelijk geen onevenredige inbreuk worden gemaakt in verhouding tot de gestelde doeleinden (proportionaliteit). Als de doeleinden bovendien op een andere wijze kunnen worden verwezenlijkt die minder nadelig is voor de betrokkenen, dan is het betreffende cameratoezicht niet toegestaan (subsidiariteit).

In de regeling is *nog* niets opgenomen over:

- Hoe de werkgever de betrokken werknemers achteraf informeert over het gebruik van de verborgen camera.
- De uitvoering van een data protection impact assessment (DPIA) voor de inzet van heimelijk cameratoezicht. De werkgever moet hiervoor altijd een DPIA uitvoeren. Ook als het heimelijk cameratoezicht incidenteel is.
- De rol van de FG is ook niet opgenomen in deze regeling. De FG dient advies te geven over de uitkomst van de DPIA en de vraag of er voldoende maatregelen zijn genomen om de risico's te beperken.

Indien de FG negatief adviseert is er sprake van een schending van de subsidiariteit en proportionaliteit en is heimelijk cameratoezicht niet toegestaan. Dit staat los van de discretionaire bevoegdheid van het CvB.

Daarnaast heeft de COR de volgende opmerkingen:

Een groot zorgpunt voor de COR is dat tussen het inzetten van ICT-faciliteiten ten behoeve van onderwijs, onderzoek en bedrijfsvoering aan de ene kant en het verantwoord en veilig gebruik van de ICT-faciliteiten en de privacy van de medewerkers/studenten aan de andere kant, vooral de taakbelasting van de medewerkers moet worden meegenomen in de uitwerking van het Privacybeleid, wanneer deze extra maatregelen voor dat veilige en verantwoorde gebruik van de ICT-faciliteiten voor extra werklust zorgen en aan de medewerkers worden opgelegd.

De COR verneemt verder graag hoe het cookiestatement van de UvA wijst op derde partij advertentie cookies, zonder toelichting over hoe deze derde partijen passen in het privacy statement van de UvA.

In het informatieveiligheidsdocument zoals dat wordt beschreven mist de COR een risicoanalyse voor de UvA als geheel. Kan de bestuurder uitleggen hoe hierin wordt voorzien?



Ons kenmerk  
cor18u/020

Graag wijst de COR ten slotte nogmaals op het uitgebreide advies van Wárlám Legal. De COR verwacht dat bij de nadere uitwerking van het Privacybeleid en het Camerareglement in concrete procedures voor de werknemers de gegeven adviezen in acht worden genomen.

Hoogachtend,

Breannán Ó Nualláin,  
Voorzitter

Maarten Terpstra,  
DB-lid