



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
16 januari 2018

Telefoon
020 525 6955

Uw kenmerk
2016cu0610

Contactpersoon
E.B.I. Moors

Bijlagen
-

Ons kenmerk
cor18/u004

Onderwerp
Informatiebeveiligingsbeleid

Geacht College,

De COR heeft op 6 april 2016 het instemmingsverzoek aangaande het informatiebeveiligingsbeleid ontvangen. Bij de aanbieding bleken echter diverse bijlagen en achterliggende stukken te ontbreken. De COR heeft direct aangegeven het instemmingsverzoek niet in behandeling te kunnen nemen, zolang deze stukken niet aangeleverd zouden worden. De COR dankt het College voor het alsnog sturen van deze stukken, maar betreurt dat dit met een grote vertraging is gebeurd. De COR heeft daarbij een aantal zorgen die maken dat hij niet instemt; ze worden hieronder uiteengezet.

De COR is niet gerust over het beleidsdocument en de bijbehorende stukken. Zo is de bedoeling van het document niet duidelijk. Het wekt de indruk voornamelijk de universiteit van juridische rugdekking te voorzien. Verder is de inhoud zeer technisch en is het moeilijk om een verband te leggen tussen het document en de praktijk. Het informatiebeveiligingsbeleid van de Universiteit Twente¹ is bijvoorbeeld korter, begrijpelijker en met een duidelijker doel geschreven, namelijk het informeren van de werknemer.

De COR vindt het ook bezwaarlijk dat de Europese privacy verordening (AVG) niet in het informatiebeveiligingsbeleid geadresseerd wordt en dat de nulmeting voor de invoering van de AVG nog moet plaatsvinden. De AVG is in april 2016 vastgesteld waarbij duidelijk was dat de UvA op 25 mei 2018 aan de AVG moet voldoen. Het baart de COR zorgen dat de UvA in de tussengelegen periode zich amper heeft voorbereid op deze wijzigingen met als mogelijk gevolg boetes. Tevens bevat de wet strengere regels voor de verwerking van persoonsgegevens, deze worden echter niet geadresseerd in dit voorgenomen beleid.

In uw antwoord op onze vragen geeft u aan dat de nulmeting bepalend is voor de mogelijke wijzigingen in het informatiebeveiligingsbeleid. De COR raadt SURFaudit² aan als instrument bij de nulmeting die ook door andere universiteiten gebruikt is. Verder gaat de COR ervan uit dat hij bij mogelijke wijzigingen in het informatiebeveiligingsbeleid een nieuw instemmingsverzoek zal ontvangen. Op grond van artikel 27 van de WOR heeft de OR namelijk instemmingsrecht wanneer de werkgever zich voorneemt een regeling vast te stellen, te wijzigen of in te trekken (i) omtrent het

¹ <https://www.utwente.nl/nl/sb/beleidssterreinen/universitair-informatiemanagement/informatiebeveiliging/>

² <https://www.surf.nl/diensten-en-producten/surfaudit/index.html>

Ons kenmerk
cor18/u004

verwerken alsmede de bescherming van persoonsgegevens van de in de onderneming werkzame personen; (ii) inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen (personeelsvolgsystemen).

De COR zou daarnaast graag een Chief Information Security Officer (CISO) aan de UvA willen zien. De CISO is verantwoordelijk voor het implementeren van, en toezicht houden op het informatiebeveiligingsbeleid binnen de Universiteit. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet daarbij voldoen aan de Baseline, een set van organisatorische en technische beveiligingsmaatregelen die geïmplementeerd en beheerd dienen te worden. De COR hecht eraan dat bij de benoeming van een CISO deze persoon volledig is vrijgemaakt voor deze taak en een organisatie-brede kijk op beveiliging heeft. Achteraf beveiliging 'inbouwen' is moeilijk, en in ieder geval duurder dan dit meenemen bij ontwerp en invoering.

De COR vindt verder dat er veel verantwoordelijkheid naar de werknemer wordt geschoven in het informatiebeveiligingsbeleid. Indien er niet aan de regels wordt gehouden, kunnen er sancties volgen en kan de werknemer aansprakelijk worden gesteld. De voorliggende ICT-gedragsregels vereisen een onderscheidend vermogen om te zien welke handeling schadelijk zou kunnen zijn. De gemiddelde werknemer heeft dit onderscheidend vermogen echter niet. Daarnaast is het aansprakelijk stellen van de werknemer in strijd met artikel 1.17 van de CAO. Werknemers zijn niet aansprakelijk voor schade, tenzij de schade een gevolg is van opzet of bewuste roekeloosheid, wat de werkgever moet kunnen aantonen. Daarom zijn de ICT-gedragsregels cruciaal. De COR vindt actualisering van de ICT-gedragsregels raadzaam, omdat die in de huidige vorm niet goed te begrijpen zijn. De COR raadt hierbij opnieuw aan de stukken van de Universiteit Twente na te gaan.

De COR is tot slot verheugd dat de pilot van de bewustwordingscampagne breder wordt uitgerold. De COR ziet graag dat er middelen beschikbaar gesteld worden om voorlichting en trainingen te geven aan de werknemers.

Hoogachtend,



Cees Kleverlaan,
Vicevoorzitter



Maarten Terpstra,
DB-lid