



**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  
2 oktober 2017  
Contactpersoon  
E.B.I. Moors

Telefoon  
020 525 6955  
Bijlagen  
-

Uw kenmerk  
2017cu1075  
Ons kenmerk  
cor17/u046

Onderwerp  
Uw brief inzake Digitalisering P-processen en P-dossiers

Geacht College,

Dank voor uw brief van 17 juli jl. (kenmerk 2017cu1075) waarin u reageert op onze eerdere brief van 21 juni jl. (kenmerk cor17/u031) waarin de COR te kennen geeft niet in te stemmen met het voorstel Project Digitalisering P-processen en P-dossiers.

In uw reactie ten aanzien van de 'Regeling toegang en beheer digitale personeelsdossiers' geeft u aan dat u de artikelen 3 t/m 13 heeft toegevoegd als bijlage. De COR komt tot de conclusie dat een aantal punten hierbij niet afdoende is opgepakt. De COR dringt zodoende toch aan om de volgende artikelen aan de 'Regeling toegang en beheer digitale personeelsdossiers' toe te voegen.

Volgens artikel 6 van de 'Regeling toegang en beheer digitale personeelsdossiers' hebben betrokkenen het recht om kennis te nemen van hun gegevens en om te verzoeken deze te laten verbeteren of te laten verwijderen. Tevens hebben zij er recht op om bezwaar te maken tegen het verwerken van persoonsgegevens. Bezwaar maken komt echter niet voor in de regeling of in de bijlage. Daarnaast wordt er geen termijn genoemd wanneer er namens het CvB besloten wordt. Zodoende wil de COR dat hier een termijn van vier weken wordt gesteld.

De COR stelt de volgende bezwaarprocedure voor:

1. Bij twijfel over het toevoegen, verwijderen, verbeteren of afschermen van stukken aan het personeelsdossier vindt eerst overleg plaats tussen P&O, PSA en DIV.
2. Bij een weigering om conform een verzoek van de medewerker (artikel 9, lid 1 en artikel 11, lid 2) te handelen ontvangt de medewerker binnen vier weken na ontvangst van het schriftelijk verzoek een gemotiveerd advies hierover van de personeelsadviseur.
3. De medewerker kan vervolgens het verzoek voorleggen aan het bevoegd gezag.
4. De door het bevoegd gezag op dergelijke verzoeken te nemen beslissingen worden gekwalificeerd als besluit in de zin van de Algemene wet bestuursrecht (Awb) waartegen de werknemer bezwaar kan maken bij het College van Bestuur.

Daarnaast wil de COR dat de volgende punten in artikel 6 worden opgenomen:

Ons kenmerk  
cor17/u046

- De betrokkene kan verzoeken om correctie van op hem betrekking hebbende persoonsgegevens, als deze feitelijk onjuist zijn, voor de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel in strijd met een wettelijk voorschrift.
- De verantwoordelijke bericht de betrokkene schriftelijk binnen vier weken na ontvangst van het schriftelijke verzoek tot correctie of aanvulling en in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed.
- De verantwoordelijke draagt zorg dat een beslissing tot correctie zo spoedig mogelijk wordt uitgevoerd.

In artikel 7 van de 'Regeling toegang en beheer digitale personeelsdossiers' wordt er gesproken over derden. De COR vraagt zich af wie deze derden kunnen zijn, naast de Belastingdienst en de accountant. De COR wil dat de werknemer specifiek toestemming geeft voor verstrekking van persoonsgegevens aan derden en stelt voor dat het volgende artikel aan de regeling wordt toegevoegd:

- Op grond van de doeleinden en de rechtmatige grondslag kunnen door of namens de verantwoordelijke persoonsgegevens worden verstrekt aan derden, mits de bewerker hiervoor schriftelijk toestemming heeft van de betrokkene, en de beheerder hier vervolgens schriftelijk toestemming voor heeft verleend.

De COR mist daarnaast nog steeds een artikel over de auditlog voor werknemers, zoals verzocht in de OV d.d. 27-01-2017. De betrokkene (dat is de persoon wiens persoonsgegevens worden verwerkt) moet kunnen overzien door wie en voor welk doel zijn gegevens worden verwerkt. De werknemer moet kunnen zien wie er in zijn dossier heeft gekeken en deze zogenaamde auditlog moet in het systeem voor de medewerker zichtbaar zijn, in plaats van deze zelf te moeten opvragen. De medewerker moet inzicht hebben wie er in zijn digitale personeelsdossier kijkt, aangezien het digitale personeelsdossier overal en altijd opvraagbaar is voor de geautoriseerde en de Autorisatiematrix relatief ruim toegang biedt.

Verder vond en vindt de COR dat de beveiliging van de gegevens van de medewerkers niet gewaarborgd is. De COR heeft in het bijzonder twee tekortkomingen geïdentificeerd.

Gegevens worden onversleuteld uitgewisseld tussen SAP en SAP-GUI. Deze gegevensuitwisseling vindt weliswaar plaats alleen binnen het UvA-netwerk maar toch zou een bekwame kwaadwillende die al toegang heeft tot het UvA-netwerk zonder veel moeite toegang tot vertrouwelijke persoonsgegevens kunnen verschaffen. En let wel, het dagelijkse aantal mensen met toegang tot het UvA-netwerk loopt in de tienduizenden. In uw brief geeft u aan geen aanleiding te vinden dit euvel te verhelpen. Hier kan de COR zich niet in vinden.

In uw recente brief schrijft u dat de COR zou hebben aangegeven dat het UvA-netwerk voldoende veiligheid biedt voor het gebruik van digitale P-processen binnen het netwerk. Dit is een misvatting van onze constatering dat onversleutelde uitwisseling van persoonsgegevens binnen het UvA-netwerk minder ernstig is dan buiten dat net. Er kan nooit sprake van voldoende veiligheid zijn waar het gaat om onversleutelde uitwisseling van persoonsgegevens waar onbevoegden toegang hebben.

Nog zwaarwegender is de problematiek rondom de VPN-oplossing in gebruik om medewerkers die zich buiten het UvA-netwerk bevinden P-dossiers te laten raadplegen. In de brief van 21 juni heeft de COR de gevaren van deze VPN-software uiteengezet. Toch vindt u wederom dat er geen aanleiding is om extra veiligheidsmaatregelen te treffen. Om de al gegeven redenen kan de COR zich hier niet in vinden.



Ons kenmerk  
cor17/u046

Bovendien bevreemdt het de COR dat u in uw brief niet verwijst naar de eerder gedane toezeggingen door de toenmalige directeur ICTS die niet zijn nagekomen.

Verder heeft de COR kennis genomen van de brief van de Senaat van 12 juli jl. waarin hij zijn 'grote bezorgdheid' over gegevensbescherming op onze universiteit uit. De COR deelt deze grote bezorgdheid en is uiterst verbaasd over de nonchalante houding ertegenover die blijkt uit uw brief.

Om de bovenvermelde redenen stemt de COR wederom niet in met de Digitalisering P-processen en P-dossiers.

Met vriendelijke groet,

Breannán Ó Nualláin,  
Voorzitter

Maarten Terpstra,  
DB-lid