UNIVERSITEIT VAN AMSTERDAM

Centrale Ondernemingsraad

COR-secretariaat

Spui 21
1012 WX Amsterdam
Postbus 19268
1000 GG Amsterdam

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

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

Datum	Telefoon	Uw kenmerk
15 november 2019	020 525 6955	2019cu1026
Contactpersoon	**Bijlagen**	**Ons kenmerk**
E.B.I. Moors	2	cor19/u036

Onderwerp
Reactie op antwoordbrief inz. Office365

Geacht College,

Op 29 oktober jl. ontvingen wij een schriftelijk antwoord op onze vragen over O365 en SURFdrive. In de Overlegvergadering van 1 november hebben we dat antwoord besproken, en heeft u ons verzocht onze bezwaren en verzoeken opnieuw schriftelijk toe te zenden. Hierbij vindt u de schriftelijke weergave van onze reactie op punten, zoals die grotendeels tijdens de OV aan bod is gekomen. Het gaat om de volgende vier punten, waarvan het tweede uit de aard van de zaak een zeer uitgebreide bespreking verdient; uitwerking van dit punt vindt u daarom apart in bijlage 1. Het vierde punt betreft de rechten van de COR, ook de gedetailleerde reactie daarop is in een bijlage ondergebracht, bijlage 2.

I Voortzetting SURFdrive en evaluatie in 2022

Ten eerste bespraken wij tijdens de OV de voortzetting van SURFdrive tot een evaluatie in 2022. Zoals ook in de brief van ICTS wordt genoemd, heeft het College toegezegd om SURFdrive te blijven aanbieden tot 2022, waarna de noodzaak tot het gebruik daarvan opnieuw moet worden geëvalueerd. De COR vindt het aanhouden van SURFdrive een goed idee. De gestelde datum voor de evaluatie lijkt ons evenwel wat vroeg, voor zover het gaat om de gevolgen van het gebruik van O365 vast te stellen. De contracten met Microsoft zijn immers van veel langere duur, en daardoor zal een prijsvergelijking op deze korte termijn niet zinvol zijn. Ook is het de COR niet bekend hoe het implementatietraject van O365 is gepland en of dat in 2022 compleet zou zijn.

Daarom stellen wij voor om de beslissing om SURFdrive al dan niet uit te faseren na 2022 ten tijde van de evaluatie in 2022 ter instemming aan de COR voor te leggen. Op deze manier kan de COR nu onafhankelijk van dreigende afschaffing van SURFdrive zijn positie ten aanzien van invoering van O365 bepalen.

II Correcties en aanvullingen t.a.v. de reactie d.d. 29/10

Multi-factor authenticatie (MFA)
In de eerste alinea op p. 1 en op p. 3 van het antwoord van 29 oktober wordt opgemerkt dat SURFdrive geen multi-factor authenticatie en geen versleuteling zou ondersteunen. Dit is onjuist. Een simpele zoekopdracht op internet geeft een complete pagina over “SurfSecureID”

(https://www.surf.nl/surfsecureid-diensten-extra-beveiligen-met-tweefactorauthenticatie). SURFdrive kent dus wel degelijk MFA waarbij een wachtwoord wordt gecombineerd met een sms of usb-sleutel. Het is vreemd dat ICTS niet op de hoogte is van deze mogelijkheden.

Daarnaast wordt gesteld dat nu reeds multi-factor authenticatie wordt gehanteerd aan de UvA, waarbij Zelfbediening als voorbeeld wordt genoemd. Zelfbediening is in elk geval voor de medewerkers die deze brief schrijven weliswaar uitsluitend toegankelijk via een VPN-verbinding, maar vereist geen andere bevestigingsbron en vraagt geen andere informatie dan het UvANetID om toegang te verschaffen. In onze ervaring is er op dit moment geen MFA. Veel server applicaties, zoals UvANose/DataNose, Canvas en SAP blijven bovendien buiten de MFA vormen van Microsoft.

De COR zou graag vernemen hoe MFA wordt ingericht, en hoe ver de invoering daarvan op dit moment is.

Privacy
Het antwoord geeft een aanbeveling over de zogenaamde “Connected Controller Experiences” (CCE): de Functionaris Gegevensbescherming (FG) beveelt aan om CCE aan te laten staan, omdat gebruikers anders naar minder veilige alternatieven gaan zoeken op internet. Dit laatste staat haaks op de aanbeveling die in de DPIA notitie over O365, juli 2019 door de Rijksoverheid wordt genoemd (zie https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise). Deze aanbeveling is daarom vreemd, waar deze ingaat tegen Rijksoverheidsbeleid.

De COR adviseert om hierover helderheid te verschaffen door een toelichting te vragen van zowel de FG als ICTS. Tijdens het overleg met ICTS en SURF werd bovendien aangegeven dat de UvA voorloopt op de Rijksoverheid met de totstandkoming van de privacy verbeteringen aan O365. Gegeven bovengenoemde afwijkende positie ten aanzien van gebruik van O365 zou de COR graag een Rijksoverheid document zien waaruit blijkt dat ook deze meent dat ICTS als koploper op het juiste spoor zit.

Functionele voordelen van O365 (zie bijlage 1 voor gedetailleerde onderbouwing)
Wat betreft de specifieke functionaliteiten van O365, en de compatibiliteit met andere hard- en software hebben wij een aantal gegevens verzameld, die ofwel ongenoemd blijven ofwel in tegenspraak lijken met de informatie in de reactie op onze brief. In de bijlage vindt u een gedetailleerde bespreking van niveau van encryptie, te verwachten problemen met O365 functionaliteit, publieke waardering van de Client functionaliteit en de (in)compatibiliteit met niet-Microsoft producten (zie bijlage 1).

Indien we afgaan op deze gegevens, dan lijkt ons de beperking van de digitale werkomgeving van alle UvA-medewerkers tot O365 sterk onwenselijk. In de reactie van 29 oktober wordt als argument voor een dergelijke beperking onder meer 'het streven naar vereenvoudiging van het IT landschap' genoemd.
Hoewel vanuit ICTS de wens van een enkelvoudige digitale omgeving begrijpelijk is, betekent enkelvoudigheid niet dat het beleid eenvoud voor alle medewerkers bewerkstelligt. De situatie is nu dat werknemers ook eigen laptops met andere bestuurssystemen moeten gebruiken, dat de aard van de onderzoeksdata of de in het onderzoeksveld gebruikelijke software hen noopt tot het gebruik van andere software en dat samenwerking breed gedeelde schijven afdwingt.
Niet alleen zouden sommige medewerkers gedwongen zijn bestaande documenten een andere naam te geven alvorens deze te verhuizen; ook zouden zij soms gedwongen zijn andere software te gebruiken.

Daarmee zijn voor hen sommige functionaliteiten niet meer beschikbaar. In de bredere context van hun werk zouden zij daarom meer problemen ondervinden.

Het schriftelijke antwoord op onze eerdere brief schetst naar onze mening op bovengenoemde zaken een onjuist beeld. Dat wekt de indruk dat er geen sprake is van een afgewogen beslissing wat betreft de gevolgen op de werkvloer. In de hoop een gezamenlijk weloverwogen oordeel op de overgang naar O365 mogelijk te maken wil de COR graag twee externe deskundigen uitnodigen, in gezamenlijk overleg aan te wijzen, om nadere toelichting te geven op de wijzigingen en de te verwachten problemen binnen de UvA.

III Financiële overwegingen

In de schriftelijke reactie wordt gesteld dat er "zeer zeker" ook beheerskosten van O365 zullen zijn, maar dat deze lager liggen dan de huidige kosten. In de conceptbegroting is wel voor het implementatietraject voor het komende jaar een bedrag van 3,2 M€ opgenomen. Wij zijn verbaasd dat de structurele beheerskosten niet nader zijn gespecificeerd, en wij hebben daarom geen goed beeld van hoe deze kosten zich precies verhouden tot de huidige kosten.

Verder begrijpen wij dat de besparing van 78.000€ per jaar op de gehele UvA begroting die het afstoten van SURFdrive zou opleveren, niet te verwaarlozen is. Zoals besproken tijdens de OV, heeft het echter ook grote voordelen om enige onafhankelijkheid te kunnen betrachten ten aanzien van de grote Amerikaanse techbedrijven. In dat licht lijkt dit bedrag een kleine prijs. Naast deze praktische overweging zou de COR het toejuichen indien het College de tijdens de OV kort door de rector geschetste visie verder zou uitwerken, en bijvoorbeeld zou besluiten financiering vrij te maken voor verder onderzoek naar de mogelijkheid van grootschaliger eigen databeheer in Nederlands of Europees verband.

Onafhankelijk van de kosten voor SURFdrive wil de COR graag een uitgewerkte raming van de kosten zien alvorens in te stemmen met de algehele migratie naar O365. In het bijzonder zouden wij graag een specificering van de kostenposten, planning van de implementatie en een raming van de te verwachten terugkerende kosten, zoals mailserverbeheer en -beveiliging, ontvangen.

IV Rechten van de COR (zie bijlage 2 voor gedetailleerde onderbouwing)

Op grond van de in ons eerdere schrijven genoemde moverende redenen houden wij vast aan ons standpunt inzake het instemmingsrecht van de COR op het besluit O365 in te voeren.

Met de omschrijving van de nieuwe systemen door ICTS wordt opnieuw bevestigd dat invoering daarvan voorzieningen betreft met nieuwe mogelijkheden tot controle en observatie van werknemers, waarin persoonsgegevens verzameld, verwerkt en bewaard worden, en waardoor de werkwijze verandert voor specifieke groepen werknemers (zie bijlage 2).

Dat het de bedoeling is dat dergelijke systemen op een verantwoordelijke manier zullen worden ingezet en dat het gebruik onder de geldende regels valt, maakt de brief ook duidelijk. In hoeverre de nieuwe mogelijkheden van O365 door die regels worden afgedekt, is ons echter nog niet duidelijk, en ook is ons niet duidelijk op welke wijze eventuele toekomstige ingebruikname van functionaliteiten binnen deze voorziening, zoals het in de brief genoemde *Delve,* aan de medezeggenschap zullen

worden voorgelegd. In onze optiek moeten al deze opties nu ter instemming worden voorgelegd, en moet een correcte procedure worden afgesproken voor medezeggenschap bij het in gebruik nemen van de functionaliteiten die de nieuwe voorzieningen bieden ter waarneming en controle van de werknemers.

De COR blijft dan ook bij zijn standpunt dat om instemming moet worden gevraagd bij het voorliggende besluit om Office365 en aanverwante functionaliteiten in te voeren. Wij hechten buitengewoon veel waarde aan instemming op dit punt, en spreken nogmaals het verzoek uit om de beslissing tot invoeren van Office365 aan de raad voor te leggen.

De COR ziet graag uw reactie tegemoet.

Hoogachtend,

Gerwin van der Pol,
Voorzitter

Cees Kleverlaan,
Vicevoorzitter

Ons kenmerk
cor19/u036

BIJLAGE 1:

Afwegingen voor- en nadelen gebruik O365, afwijkend van het geschetste beeld

Encryptie
Wat betreft encryptie lijkt er sprake te zijn van een semantische discussie. SURF gebruikte tot voor kort geen "self encrypting" disksystemen, dus in die zin kun je inderdaad spreken van een ontbreken van encryptie. Dergelijke systemen zijn van belang om te waarborgen dat bij vernietiging van de systemen werknemers van het vernietigingsbedrijf de disks in geen geval kunnen lezen (Microsoft noemt dit Disk Level Encryption).

Toch is dat niet het belangrijkste aspect in deze discussie waar het meer over lijkt te gaan over encryptie van bestanden. Voor de encryptie van bestanden op SURFdrive kan zeer eenvoudig zorg worden gedragen door inzet van een aantal betrouwbare encryptie software systemen. Voordeel van een dergelijk systeem is dat de gebruiker zelf de sleutel in handen heeft voor versleuteling. Dat SURFdrive geen encryptie heeft is derhalve een onjuiste weergave van feiten. De gebruiker heeft alle mogelijkheden daartoe en wordt daartoe ook aangespoord (zie bijvoorbeeld: https://www.surf.nl/bewaar-en-deel-je-bestanden-veilig-in-de-cloud-met-surfdrive/veelgestelde-vragen-over-surfdrive).

Bij de twee encryptie lagen die Microsoft omschrijft naast de Disk level encryptie vallen enige vraagtekens te plaatsen. Er zijn diverse software lagen waar Microsoft wellicht claimt dat alles prima qua veiligheid op orde is, maar waar in de afgelopen jaren ook de nodige problemen zijn geweest. Een paar voorbeelden: TLS (Transport Layer Security) wordt door veel mail clients gebruikt, maar heeft afgelopen jaren laten zien dat diverse kwetsbaarheden tot inbraak konden leiden (zie bijvoorbeeld https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=TLS). Vooralsnog is met versie 1.4 alles weer op orde tot de volgende kwetsbaarheid weer boven water komt. Dit geldt overigens zeker niet alleen voor Microsoft producten, maar ook voor diverse alternatieven.

Een typisch Microsoft encryptie systeem dat verbonden is met O365 is de O365 Message Encryption (OME). Deze methode lijkt op orde te zijn maar gebruikers moeten ook hier expliciet aangeven hun berichten te willen versleutelen. Vervelender is dat de sleutels voor deze encryptie in handen zijn van Microsoft. Het is vergelijkbaar met het afgeven van je kostbare spullen bij een bank met het vertrouwen dat de bank er goed voor zorgt. Dat alle bankmedewerkers erbij kunnen, neem je dan kennelijk voor lief, maar het betekent ook dat "bezoekers" van die bank die niet voldoende afgesloten deuren open hebben gekregen ook bij je spullen kunnen. In dat geval is het beter wanneer er een kluis is die op slot gaat met een sleutel die niet bij Microsoft ligt, maar onder je hoofdkussen thuis.
Microsoft heeft niet bepaald de naam opgebouwd dat hun systemen uitblinken door veiligheid; dat heeft er enerzijds mee te maken dat de grote hoeveelheid gebruikers van de Microsoft software deze tot gewild object van inbraak maken van met name buitenlandse spionage partijen, anderzijds echter ook door keuze van een monolithische opbouw van hun software producten waardoor een escalatie van gebruikersrechten kan plaatsvinden en de schade potentieel zeer grote omvang kan krijgen.
Met name dit laatste kan ook het geval zijn bij O365 waar vele producten met verschillende gebruiksingangen (mobiel, desktop, laptop, ipad met verschillende besturingssystemen) een potentieel risico vormen. Wanneer we het lijstje van zeer urgente software kwetsbaarheden van afgelopen paar jaar (CVE vulnerabilities) bestuderen kunnen we concluderen dat Office en Outlook-achtige software regelmatig in de rode categorie is beland van urgente kwetsbaarheden.

Door nu zulke belangrijke services als onze mail en de gezamenlijke schijven onder te brengen in de Microsoft Cloud omgeving wordt de verantwoordelijkheid ogenschijnlijk bij Microsoft gelegd voor beveiliging. Naar de mening van de COR is dat het ontlopen van verantwoordelijkheid. De COR zou er een voorstander van zijn om een encryptie-sleutel te gebruiken die alleen binnen de UvA kan worden gekend.

Teams functionaliteit
Veel zaken van O365 vallen onder het kopje “Teams” waar bijvoorbeeld het samenwerken aan documenten, calendars en vele andere zaken onder vallen. Het betreft in feite zaken waar veel medewerkers al lang via alternatieve wegen kennis mee hebben gemaakt en dan ook zullen vergelijken met het gedrag van O365. Getuige veel opmerkingen op internet is de performance van O365 voor gezamenlijk bewerken van documenten niet bijster goed. Op bepaalde UvA locaties is momenteel Slack (https://slack.com/) populair bij groepen medewerkers (m.n. bij bijvoorbeeld PhD’s in experimentele groepen om te communiceren tussen werkplek en lab). Het Microsoft “slack” alternatief voor chats wordt regelmatig als “onbruikbaar“ gewaardeerd (zie bijv. https://news.ycombinator.com/item?id=19625514). De reden hiervoor is de zeer slechte real-time performance van Microsoft Teams: er treedt vertraging in de communicatie op. Bovendien is installatie van O365 op experimentele PC’s in veel gevallen niet logisch. Een en ander betekent dat medewerkers hoogstwaarschijnlijk bij voorkeur doorgaan met die applicaties waar ze een positieve ervaring mee hebben en niet de O365 equivalenten zullen willen hanteren.

Client functionaliteit
Sinds de laatste Apple update lijkt de Onedrive applicatie nu zonder problemen te installeren. Dat laat onverlet dat Onedrive diverse zaken van Apple of Linux niet ondersteunt: bijvoorbeeld filenamen die beginnen met een punt. Dat lijkt voor Windows gebruikers misschien onbelangrijk, maar voor Apple en Linux vormen dat essentiële filenamen. Het gaat in die systemen namelijk om verborgen files die voor tal van instellingen worden gebruikt. Een en ander heeft te maken met de eerder genoemde restricties op filenamen die Microsoft hanteert. Het volledige pallet aan mogelijke karakters wordt door Microsoft *niet* ondersteund; dat heeft veel nadelige gevolgen voor niet-Windows gebruikers.

Compatibiliteit niet-Microsoft producten
In de brief wordt niet ingegaan op de problemen van communicatie tussen Microsoft producten en alternatieve programma's. Zo leidt het versturen van een agenda-uitnodiging vanuit een Apple-agenda naar een Outlook-agenda tot een uitnodiging op een foutief tijdstip. Het gebruik van alternatieve browsers als Safari of Firefox leidt soms tot het niet kunnen lezen van pop-ups, een vreemde vormgeving en het verdwijnen van functionaliteiten. Aangezien dergelijke programma's ook veelvuldig binnen de UvA worden gebruikt, is onderzoek naar compatibiliteit zeer gewenst.

BIJLAGE II

Rechten COR, overwegende de aard van de nieuwe voorzieningen, verwerking persoonsgegevens en werkwijze.

In de reactie d.d. 29 oktober wordt bevestigd dat het besluit rond de invoering van O365 precies die zaken betreft die ter instemming aan de COR moeten worden voorgelegd. Ter aanvulling op de argumentatie die wij eerder gaven in onze brief d.d. 11 oktober en bij wijze van toelichting bespreken wij enkele punten uit de brief:

- Microsoft is verwerker en "handelt conform de AVG-richtlijnen en handelt op instructie van de verwerkingsverantwoordelijke volgens de in het contact [sic] bepaalde doelbindingen"(p. 6, punt 3).

Iedere nieuwe regeling omtrent verzamelen, bewaren, gebruiken, verstrekken en beveiligen van persoonsgegevens, dus die gegevens waar de AVG-richtlijnen van toepassing zijn, is instemmingsplichtig. In dit contract wordt een nieuwe regeling vastgelegd ten aanzien van rechten en plichten rond het gebruik van persoonsgegevens van UvA-werknemers.

-Logging en monitoring mogelijkheden zijn er nu ook [...] in die gevallen dat er functionele mogelijkheden ontstaan die kunnen worden gekenmerkt als mogelijkheden tot waarneming en controle van het gedrag van medewerkers, dan vindt hierover aparte besluitvorming plaats (p. 6, punt 1).

De 'aparte besluitvorming' over het hanteren van voorzieningen die deze mogelijkheden bieden is inderdaad nu aan de orde. In dit geval betreft het nieuwe voorzieningen, namelijk nieuwe servers, een nieuwe cloudvoorziening, nieuwe registratie van het gebruik van software, mailverkeer en documentopslag en het door een nieuwe partij uitgevoerde beheer, die 1) persoonsgegevens op een nieuwe manier verzamelen, bewaren, gebruiken, verstrekken en beveiligen en 2) nieuwe mogelijkheden tot de waarneming en controle van het gedrag van de werknemer bewerkstelligen. Zoals gesteld in de brief, is in het contract vastgelegd dat (p. 2):

1 Microsoft verwerkt de verzamelde gegevens [...]
2 dit geldt [...] voor [...] gegevens over het individuele gebruik van de diensten

Tot op heden bestond deze specifieke dataverzameling niet voor de groep werknemers die de digitale werkomgeving van O365 zal moeten gaan gebruiken. Gegevens rond het individuele gedrag van de werknemers, namelijk het gebruik van de aangeboden diensten, nieuw of niet voor de betreffende werknemer, worden nu actief en als nieuwe verzameling door Microsoft verwerkt. Er wordt gesteld dat het contract het gebruik van deze data beregelt, aangezien het ook vastlegt dat (p. 2):

3 "Microsoft garandeert dat zij de twee inhoudelijke en diagnostische gegevens NIET gebruikt voor profilering, data-analyse, marktonderzoek en adverteren".

Dat betekent nu precies dat het contract een regeling betreft rond 1) persoonsgegevens en 2) een voorziening die waarneming en controle van het gedrag van werknemers mogelijk maakt: er wordt immers vermeld hoe in het contract met Microsoft het daadwerkelijke gebruik van die gegevens en die voorziening reguleert. Op besluiten rond dergelijke regelingen heeft de COR van de wetgever instemmingsrecht gekregen.
Verder wordt de volgende mogelijkheid genoemd:

"Binnen O365 is er een functionaliteit waarmee b.v. een eigenaar van een document kan zien wie het betreffende document geraadpleegd heeft [...] Dat kan worden gezien als een mogelijkheid ter observatie en controle." (p. 5)

De genoemde functionaliteit betekent dat invoering van de voorziening die deze mogelijkheid biedt (ook al is die mogelijkheid niet gerealiseerd) nu juist ter instemming van de COR moet worden voorgelegd.

Ten laatste wordt gesteld dat de bestaande spelregels rond ICT-voorzieningen en beheer worden toegepast (onder verwijzing naar de 'Regels voor verantwoord gebruik van ICT-faciliteiten voor de medewerkers van de Universiteit van Amsterdam' vastgesteld bij besluit nr. 2018-068316). Dat is natuurlijk geruststellend; het gaat hier echter om het besluit tot de invoering van voorzieningen waar deze regels op toe te passen zullen zijn. Zoals boven omschreven is dat een besluit waarmee de COR moet worden gevraagd in te stemmen.

- *Conclusie: [...]'O365 biedt een nieuwe, veiligere, manier van (samen-)werken aan'.*

In de brief wordt geconcludeerd dat de werkwijzen hiermee niet ingrijpend veranderen; op grond van de in bijlage 1 beschreven wijzigingen en problemen constateren wij dat dat beslist niet voor iedereen geldt, namelijk niet voor de groep medewerkers die geen gebruik maakt van Windows besturingssystemen; voor de groep die geen gebruik maakt van Office producten en voor de groep medewerkers die geen gebruik maakt van cloudservices maar gedeelde netwerkschijven. Dezen zullen aan een nieuwe werkwijze moeten beginnen, indien "het ICT-landschap" tot O365 zal worden beperkt.