Voorlegger vergadering Raad van Bestuur UWV

	Vergadering Raad van bestuur			
Datum	2 mei 2023			
Agendapunt	Agendapunt	7	Nummer	23-151
Onderwerp	Maatregelen inzake het weren van apps op mobiele devices van rijksambtenaren			
Directeur	CIO			
Opsteller	CIO			
Portefeuillehouder RvB	Nathalie van Berkel			

	Onderwerp heeft instemming van
Directeur	**Toelichting**
Directeur HRM	Akkoord
Directeur Communicatie	Akkoord

Door Raad van bestuur te nemen besluiten

Ter kennisname. De portefeuillehouder Raad van Bestuur is akkoord gegaan met de volgende besluiten:

Besluit om beleidslijn BZK te volgen en de maatregelen die zorgen dat apps op mobiele devices ook voor medewerkers UWV geweerd kunnen worden.

Bij het besluit is het volgende van belang:
- De eerste stap is het per direct aan ambtenaren in dienst UWV ontraden en af te dwingen om apps geïnstalleerd te hebben en te gebruiken op hun mobiele werkapparatuur van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen. De directie CIO rijk heeft hiervoor een handreiking gemaakt voor welke apps dit van toepassing is.
- Tegelijk zal worden toegewerkt naar de situatie waarbij mobiele apparaten, uitgereikt aan ambtenaren in dienst van UWV, zo zijn ingericht dat er alleen vooraf toegestane apps, software en/of functionaliteiten kunnen worden geïnstalleerd en gebruikt. Het worden dan in zijn geheel zogeheten 'managed apparaten', waarvoor is bepaald welke apps daarop kunnen worden geïnstalleerd en gebruikt door de gebruiker. Apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen zullen dan niet toegestaan worden.
- Indien er een noodzaak is voor de werkuitoefening om een uitzondering te vormen, zal dit apart bekeken worden en indien nodig ter besluitvorming voorgelegd.

Samenvatting onderwerp en reden bespreking

Op 2 februari 2023 zijn er schriftelijke vragen gesteld, met kenmerk 2023Z01674, door het lid Dekker-Abdulaziz (D66) over de mogelijkheid om de Chinese applicatie TikTok te weren op mobiele devices van medewerkers van de Rijksoverheid. Op basis van de vragen van de Kamer is aan de AIVD gevraagd een advies te geven. De conclusie daarvan is dat het gebruik en de aanwezigheid van mobiele telefoons en de daarop geïnstalleerde applicaties te allen tijde een inherent spionagerisico vormen. Het is daarom raadzaam altijd een grondige afweging plaats te laten vinden tussen de noodzaak van het installeren van een bepaalde applicatie enerzijds en het daarbij behorende risico anderzijds. Gebruik van apps van bedrijven uit landen met een offensief cyberprogramma door ambtenaren in dienst van de rijksoverheid[1] verhoogt dit risico. Zie voor de volledige beantwoording de brief aan de Kamer[2].

[1] Dit zijn alle ambtenaren in dienst bij de departementen en daaronder vallende agentschappen en andere uitvoeringsorganisaties.
[2] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?did=2023D11252&id=2023Z04749

In het licht van de genoemde risico's en de beschouwing van de AIVD acht de Staatsecretaris het nodig om aanvullende stappen op het gebied van veiligheid van mobiele apparaten bij de Rijksoverheid te zetten. De eerste stap is het per direct aan ambtenaren in dienst van de Rijksoverheid ontraden en af te dwingen om apps geïnstalleerd te hebben en te gebruiken op hun mobiele werkapparatuur van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen. De directie CIO rijk heeft hiervoor een eerste overzicht opgesteld van apps die worden uitgesloten van de allowlist. Het betreft een dynamisch overzicht dat niet expliciet zal worden gepubliceerd. Zie bijlage A.

➔ ***Gevraagd besluit aan de RvB is om als UWV deze richtlijn te volgen en de genoemde apps te weren op de mobiele werkapparatuur.***

Tegelijk zal op worden toegewerkt naar een situatie waarbij mobiele apparaten, uitgereikt aan ambtenaren in dienst van de rijksoverheid, zo zijn ingericht dat er alleen vooraf toegestane apps, software en/of functionaliteiten kunnen worden geïnstalleerd en gebruikt. Het worden dan in zijn geheel zogeheten '*managed apparaten*', waarvoor is bepaald welke apps daarop kunnen worden geïnstalleerd en gebruikt door de gebruiker. Apps van bedrijven uit landen met een offensief cyberprogramma tegen Nederland en/of Nederlandse belangen zullen dan niet toegestaan worden.

Uitzondering op de bovenstaande maatregelen geldt wanneer een dergelijke applicatie nodig is of kan zijn voor het uitoefenen van een primaire taak van een rijksorganisatie. Hierbij kan worden gedacht aan inspectie en toezicht, opsporingsonderzoek of inlichtingenbelang. Deze uitzondering zal in samenwerking met de departementen de komende periode verder worden uitgewerkt.

Met dit voorstel volgen we de beleidslijn voor Rijksambtenaren. Hier stellen we ons op het standpunt dat door de werkgever verstrekte apparaten voor zakelijk gebruik bedoeld zijn, waarbij we privé gebruik binnen de gedragsregels etc. toestaan. Privégebruik is echter geen recht, evenals dat we alle apparaten onder beheer van UWV ("managed") hebben, policies instellen, verbieden, resp. voorkomen en monitoren dat er geen oneigenlijk gebruik is. Dit geldt voor alle UWV-desktops en laptops en dit is voor door UWV verstrekte telefoons en tablets beleidsmatig niet anders.

Gevolgen voor mensen

n.v.t.

Kansen en risico's voor (de opdracht van) UWV

n.v.t.

Strategische aspecten van het besluit

n.v.t.

Bedrijfsvoering (personeel/financieel)

n.v.t.

Duurzaamheid

N.v.t.

Vervolgtraject besluitvorming

n.v.t

Communicatie

Op basis van een voorgenomen besluit is dit via DWU aan alle medewerkers gecommuniceerd en is ook de OR geïnformeerd. Van belang is dat we goed uitleggen wat de aanleiding is en de argumentatie waarom we een verbod instellen.

Openbaarheid

Deze documenten kunnen openbaar gemaakt worden (onderbouw ook de keuzes voor opties 2, 3 en 4):
1 ☐ Ja, in hun geheel.

2 ☐ Deels, markeer in de documenten wat niet openbaar gemaakt kan worden.
3 ☒ Nee, de bijbehorende bijlage(n) niet.
4 ☐ Nee, helemaal niet.

5.1 lid 2 sub i
