Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 200 VII Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2023

Nr. 158 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 april 2023

Op 22 december 2022 heeft de Tweede Kamer de voortgangsinformatie zoals verzonden aan de Group of States Against Corruption van de Raad van Europa (GRECO) ontvangen.[1] Drie annexen bij deze voortgangsinformatie zijn op vertrouwelijke basis aan de Kamer verstrekt. Op 24 maart jl. heeft uw commissie de Minister van Binnenlandse Zaken en Koninkrijksrelaties verzocht om een nadere motivering omtrent de vertrouwelijkheid van deze stukken.

De politieorganisatie beschikt over veel gevoelige en vertrouwelijke (opsporings)informatie. Het is dan ook belangrijk dat hier door medewerkers zeer zorgvuldig mee wordt omgegaan en dat politiesystemen zodanig zijn ingericht dat deze vertrouwelijkheid ook zoveel mogelijk wordt geborgd. Dit geldt ook voor externe uitingen over de politie en haar informatiesystemen. De politie heeft dan ook verzocht de drie annexen in kwestie vertrouwelijk aan de Kamer te verstrekken. De noodzaak daarvan licht ik hieronder per stuk nader toe. Indien uw commissie zich niet (volledig) kan vinden in deze nadere motivatie, treden wij graag met uw commissie in overleg over eventuele alternatieven.

Annex A – Always Alert (Dutch)

Dit betreft een richtlijn over het gebruik van zowel interne als externe applicaties (apps). Deze richtlijn dient om diverse redenen vertrouwelijk te worden behandeld. Ten eerste geldt dat de richtlijn inzichtelijk maakt welke apps door de politie wel en niet mogen worden gebruikt. Door dit inzichtelijk te maken, kunnen de gebruikte apps mogelijk sneller doelwit zijn van hackers. Daarbij komt dat de richtlijn inzicht geeft in de extensie voor een account dat door de politie wordt gebruikt, waardoor dit risico verder wordt vergroot. Ook is uit de richtlijn kenbaar via welke app(s)

[1] Kamerstuk 36 200 VII, nr. 155.

kst-36200-VII-158
ISSN 0921 - 7371
's-Gravenhage 2023

operationele informatie en als «Politie Geheim» gerubriceerde informatie en bestanden mogen worden gedeeld. Het is dan ook niet wenselijk dat personen die kwaad in de zin hebben, kennis kunnen nemen van deze richtlijn.

Annex I – Guidance for accessing police systems (Dutch)

Dit betreft een interne handleiding voor het raadplegen van politiesystemen. Het is van belang om informatie in dergelijke systemen goed te beveiligen en politiemedewerkers te begeleiden in hun omgang met vertrouwelijke en gevoelige (opsporings)informatie. Door personen die kwaad in de zin hebben inzicht te geven in de handleiding, kunnen zij mogelijk kwetsbaarheden ontdekken en deze misbruiken voor hun eigen doeleinden. Zo geeft de handleiding inzicht in de diverse vragen die een politiemedewerker zichzelf moet stellen en in de regels voor het vastleggen van raadplegingen van systemen. Eventueel misbruik hiervan (bijvoorbeeld het specifiek stimuleren van gedrag in strijd met de handleiding) dient zoveel als mogelijk te worden voorkomen.

Annex J – Prudently Dealing With Information (Dutch)

In dit document wordt omschreven hoe binnen de politie veilig wordt omgegaan met informatie. Hierbij wordt inzichtelijk gemaakt welke rubriceringsniveaus (politie intern tot politie zeer geheim) van toepassing zijn op specifiek genoemde bestanden, opsporingsdossiers en intern vertrouwelijke informatie. Hierbij moet gedacht worden aan bijvoorbeeld de wijze waarop wordt omgegaan met het informatie die ziet op informantenregister, getuigenbescherming en tapgesprekken. Per rubriceringsniveau wordt vervolgens inzichtelijk gemaakt hoe dergelijke informatie dient te worden getransporteerd, opgeslagen en vernietigd. Het is niet wenselijk dat personen die kwaad in de zin hebben van dit document kunnen kennisnemen en op de hoogte zijn van de mate van beveiliging. Door te weten welke veiligheidsmaatregelen zijn ingebouwd bij welk type document (bijvoorbeeld welk bestandsvercijferingsprogramma wordt gebruikt), kan mogelijk gericht worden geprobeerd deze informatie te onderscheppen met als bedoeling om hier misbruik van te maken.

Omgang GRECO vertrouwelijke informatie

U heeft tot slot de vraag gesteld hoe GRECO omgaat met vertrouwelijke informatie. Hierbij geldt dat de voortgangsinformatie en annexen slechts aan het GRECO-secretariaat en de door GRECO benoemde rapporteurs zijn verstrekt. Op deze wijze kunnen het secretariaat en de rapporteurs beoordelen of en in hoeverre de aanbevelingen zijn geïmplementeerd. Zij stellen vervolgens een nalevingsverslag op waarin dit oordeel is neergelegd en dat dient te worden goedgekeurd door de plenaire vergadering van GRECO. De door het secretariaat en de rapporteurs ontvangen voortgangsinformatie en annexen worden niet separaat openbaar gemaakt of aan de plenaire vergadering verstrekt. Hoewel het nalevingsverslag naar deze informatie kan verwijzen, zijn de bevindingen van GRECO veelal zakelijk geformuleerd en kan het land in kwestie – zoals gebruikelijk – met GRECO overleggen over welke informatie wel/niet en zo ja in welke vorm in het verslag kan worden opgenomen. Hiermee wordt ervoor gezorgd dat GRECO voor haar beoordeling over zoveel mogelijk informatie beschikt als mogelijk en haar bevindingen openbaar kan rapporteren, zonder dat hierbij vertrouwelijke informatie openbaar wordt.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius