



# Bijlage 1 - Motivering bij besluit op Woo- verzoek CAS

## Kenmerk 9601

### ALGEMEEN

Bijzonderheden over (delen van) documenten (bijvoorbeeld verwijzingen naar reeds openbare documenten, reeds beoordeeld of dergelijke) zijn vermeld in de onleesbaar gemaakte passages, evenals in de opmerkingenkolom van de inventarislijst (bijlage 2 bij dit besluit).

Voor zover uitzonderingsgronden van de Woo zijn toegepast op onleesbaar gemaakte delen van de geselecteerde documenten, is een cijfercode vermeld en/of een combinatie daarvan. Waar een combinatie van cijfercodes is toegepast op de onleesbaar gemaakte (delen van) documenten, dienen deze in onderlinge samenhang te worden gezien. De motivering voor de toepassing van de uitzonderingsgronden is hieronder opgenomen.

### Weigeringen per document(-onderdeel)

De documenten met nummers 1 tot en met 21, bevatten de speerpunten per gebied. Het Criminal Anticipation System (hierna: CAS) is een model waarmee de politie criminaliteitspatronen in kaart kan brengen. Het begrip "speerpunt" ziet in de context van het CAS, op criminaliteitsthema's die door de predictive policing techniek voor een basisteam in een specifieke tijdsperiode worden gegenereerd. De gelakte onderdelen zien op de variabelen en afkortingen die in de pythonscripts zijn opgenomen. Dit laatste geldt ook voor de documenten met nummers 76, 77, 101 tot en met 106 en alle modelbestanden. Bij openbaarmaking van deze afkortingen en variabelen kunnen hackers of kwaadwillenden de politie in de uitvoering van haar taak belemmeren en gebruiken voor de voortzetting van mogelijk criminele activiteiten. Hiermee loopt de politie het risico dat zij haar wettelijk toebedeelde taak niet meer naar behoren kan uitvoeren.

Documenten met nummers 22 tot en met 75 en 78 tot en met 100 zijn eveneens geweigerd. Deze documenten bevatten namelijk informatie wat direct inzicht geeft in de interne werking van de digitale infrastructuur van de politie. Ook hiervoor geldt dat het gevaar op sabotage en (mogelijke) verhindering van de opsporing en vervolging van strafbare feiten in het geding komen wanneer deze informatie openbaar gemaakt wordt aan eenieder.

Overeenkomstig zijn in de inventarislijst de bestandsnamen van documenten met nummers 22 tot en met 73, 86, 87, 88, 89, 90, 94, 95 en 96 gelakt. Deze bestandsnamen bevatten namelijk verwijzingen naar inhoud die vanwege de herleidbaarheid naar interne (digitale) bedrijfsprocessen niet gedeeld kunnen worden. Openbaarmaking hiervan zou tot gevolg (kunnen) hebben dat de veiligheid van deze interne processen niet gewaarborgd kan worden.

Het belang van de opsporing en vervolging van strafbare feiten, het belang van het voorkomen van sabotage en het belang van het goed functioneren van het bestuursorgaan dienen in onderhavig geval zwaarder te wegen dan het belang van openbaarmaking.

Omdat deze weigeringsgronden in samenhang moeten worden gezien en op ieder gelakt onderdeel van toepassing zijn zal, naast de zojuist gegeven motivering per document, hieronder per weigeringsgrond een diepere uiteenzetting worden gegeven.

### **Artikel 5.1, lid 2 onder c van de Woo (cijfercode 7)**

Het openbaar maken van informatie ingevolge de Woo blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen het belang van de opsporing en vervolging van strafbare feiten.

Uit de Woo kan worden afgeleid dat door de wetgever aan de in artikel 5.1 en 5.2 van de Woo beschreven uitzonderingsgronden het uitgangspunt ten grondslag is gelegd dat de politie haar wettelijke taak binnen een zekere mate van geheimhouding kan uitvoeren, waarbij zij onder bepaalde omstandigheden haar werkwijzen van opsporing en vervolging van strafbare feiten (in beginsel) geheim kan houden. Indien bepaalde onderdelen van de documenten (deels) openbaar worden, kan de politie worden belemmerd om de in het kader van artikel 3 van de Politiewet 2012 aan haar opgedragen taken uit te voeren en worden de doeleinden (op korte en lange termijn) van het stelsel van handhaving van de openbare orde en veiligheid in gevaar gebracht ofwel kunnen deze in gevaar komen.

Het CAS) is een systeem om criminaliteitspatronen in kaart te brengen. Hierdoor wordt het voor de politie inzichtelijk in welke gebieden het risico op bepaalde soorten criminaliteit het grootst is. Dit draagt bij aan de handhaving van de openbare orde en veiligheid en ziet daarmee rechtsreeks op de opsporing en vervolging van strafbare feiten. Door openbaarmaking van de gelakte onderdelen komen deze belangen in het geding. Dat leidt ertoe dat de politie gefrustreerd wordt in de uitvoering van de wettelijk aan haar opgelegde taak.

Hoewel de gelakte informatie met name ziet op de digitale infrastructuur van de politie (zie ook cijfercode 11 hieronder voor een nadere motivering), houdt dit dus rechtstreeks verband met het belang van de opsporing en vervolging van strafbare feiten waardoor deze zwaarder weegt dan het belang van openbaarmaking. Om deze reden maak ik de informatie niet openbaar.

### **Artikel 5.1, lid 2 onder e van de Woo (cijfercode 9)**

Het openbaar maken van informatie ingevolge de Woo blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen het belang van de eerbiediging van de persoonlijke levenssfeer, tenzij de betrokken persoon instemt met openbaarmaking.

Bij de afweging van het belang van de eerbiediging van de persoonlijke levenssfeer van bij de aangelegenheid betrokken natuurlijke personen, rechtspersonen dan wel derden tegenover het belang van de openbaarmaking, maak ik informatie niet openbaar die leidt (kan leiden) tot namen van personen dan wel een derde. Het openbaar maken van deze persoonsgegevens -als bedoeld in artikel 1 van de AVG- maakt of kan een inbreuk maken op de persoonlijke levenssfeer van betrokkene(n) die al dan niet in dienst zijn van de politie.

Weliswaar kan, waar het gaat om beroepshalve functioneren van politieambtenaren, slechts in beperkte mate een beroep worden gedaan op het belang van eerbiediging van hun persoonlijke levenssfeer, maar dit ligt anders indien het gaat om het openbaar maken van namen van de politieambtenaren, die geen publieke functie bekleden maar hun functie executief, binnen een project of in het kader van een (opsporings)zaak uitoefenen. Daarbij is van belang dat het hier niet gaat om het opgeven van een naam aan een individuele burger die met een ambtenaar in contact treedt, maar om openbaarmaking van de naam in de zin van de Woo. Die openbaarheid is immers niet in tijd en omvang begrensd. Namen van ambtenaren worden gezien als persoonlijke en dus te beschermen gegevens (zie bijvoorbeeld: ABRvS, 24 februari 2016, ECLI:NL: RVS:2016:445). Daar waar geen sprake is van een publieke functie, zijn de naar personen herleidbare gegevens onleesbaar gemaakt.

Wat betreft de afdelings- en/of functienamen wordt overwogen dat er sprake is van (zeer) specifieke afdelingen, waarbinnen ook (zeer) specifieke functies zijn toegekend, die leiden of kunnen leiden tot herleidbaarheid naar de betreffende (politie)ambtenaar. Als bovendien de betreffende afdeling wordt benaderd door derden en de benaderde medewerker van deze afdeling kent daarvan niet de achtergrond, kan informatie worden verstrekt over de (contact)gegevens van personen waarmee herleidbaarheid naar personen een feit is/kan worden. Hierom zijn de betreffende gegevens onleesbaar gemaakt.

Voorts merk ik op dat openbaarmaking van (indirect) naar (politie)ambtenaren herleidbare persoonsgegevens een veiligheidsrisico met zich meebrengt. Het is bekend dat medewerkers zijn bedreigd en dat privéadresgegevens van (politie)ambtenaren zijn achterhaald. Gebleken is dat (politie)ambtenaren en soms ook hun gezinsleden/familie/vrienden te maken hebben of hadden met bedreigingen (ook aan het privéadres). Het openbaar maken van namen van (politie)ambtenaren of naar hen herleidbare informatie, kan ertoe leiden dat het aantal bedreigingen toeneemt. Onder andere social media kan hier in negatieve zin een bijdrage aan leveren. Het fenomeen 'doxing', waarbij mensen actief proberen de identiteit van politieambtenaren te achterhalen en te onthullen, is een fenomeen die in negatieve zin een directe inbreuk maakt op de persoonlijke levenssfeer van de betrokkene(n) en/of op hun veiligheid.

Gelet hierop ben ik van mening dat primair het belang als bedoeld in artikel 5.1, lid 2 onder e van de Woo zwaarder dient te wegen dan het belang van openbaar maken voor eenieder van bedoelde gegevens.

#### **Artikel 5.1, lid 2 onder h van de Woo (cijfercode 11)**

Dit artikel bepaalt dat het openbaar maken van informatie eveneens achterwege blijft voor zover het belang daarvan niet opweegt tegen het belang van de beveiliging van personen en bedrijven en het voorkomen van sabotage.

Deze cijfercode is toegepast op informatie die ziet op broncodes, beheerscripts, coëfficiënten, en pythonscripts en de daarbij behorende variabelen en afkortingen die de politie hanteert voor de interne digitale infrastructuur.

Het belang om de betreffende passages niet openbaar te maken wordt onderstreept door het feit dat de niet openbaar gemaakte informatie betrekking heeft op voor de politieorganisatie belangrijke software en systemen die nog steeds worden gebruikt, zodat deze tot ver in de toekomst relevant zullen blijven. Het risico dat de gevraagde informatie na openbaarmaking voor hacks of hackpogingen (sabotage van politiestructuren) zal worden gebruikt, is daarom (blijvend) aanwezig. Nu de software en systemen cruciaal zijn voor de politie en er een risico op sabotage van de software en systemen die de bedrijven aan de politie levert bestaat, moet het risico op inbreuken hierop zoveel mogelijk worden vermeden/gemitigeerd. Het gaat daarbij om kritische ondergrenzen. Voorkomen moet worden dat derden door openbaarmaking nieuwe of aanvullende informatie krijgen waarmee zij, in combinatie met al openbare informatie of informatie waarover zij reeds beschikken, kunnen anticiperen op het optreden van de politie. De veiligheid van digitale systemen is een continu aandachtspunt en de pogingen van derden om de integriteit van digitale systemen aan te tasten, nemen in aantal toe, evenals de professionaliteit waarmee die pogingen worden ondernomen. Het verstrekken van de onder deze cijfercode vallende informatie blijft daarom ook achterwege.

Het feit dat de documenten ouder dan vijf jaar zijn doet aan het bovenstaande niet af, nu de genoemde software en systemen nog steeds worden gebruikt door de politie.

#### **Artikel 5.1, lid 2 onder i van de Woo (cijfercode 12)**

Het openbaar maken van informatie ingevolge de Woo blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.

Deze cijfercode is toegepast op informatie die ziet op onderdelen gerelateerd aan de digitale infrastructuur van de politie. Openbaarmaking van deze informatie staat de opsporing en vervolging van strafbare feiten in de weg en maakt de politie kwetsbaar voor kwaadwillenden zoals hackers, hetgeen het goed functioneren van het politieapparaat en daarmee ook dat van de Staat, belemmert of zou kunnen belemmeren.

Het belang deze passages niet openbaar te maken wordt, evenals de onder cijfercodes 7 en 11 opgenomen belangen, onderstreept door het feit dat de niet openbaar gemaakte informatie

betrekking heeft op voor de politieorganisatie belangrijke software en systemen, die nog steeds worden gebruikt, zodat deze tot ver in de toekomst relevant zullen blijven. Het risico dat de gevraagde informatie na openbaarmaking voor hacks of hackpogingen zal worden gebruikt, is daarom (blijvend) aanwezig. Nu de software en systemen cruciaal zijn voor het goed functioneren van de politie, moet het risico op inbreuken op de beveiliging zoveel mogelijk worden vermeden/gemitigeerd. Het gaat, zoals eerder ook aangegeven, daarbij om kritische ondergrenzen. Voorkomen moet worden dat derden door openbaarmaking nieuwe of aanvullende informatie krijgen waarmee zij, in combinatie met al openbare informatie of informatie waarover zij reeds beschikken, kunnen anticiperen op het optreden van de politie of de toepassing van de methoden en technieken kunnen frustreren. De veiligheid van digitale systemen is een continu aandachtspunt en de pogingen van derden om de integriteit van digitale systemen aan te tasten, nemen in aantal toe, evenals de professionaliteit waarmee die pogingen worden ondernomen.

Voor zover de informatie inzicht biedt in de voorwaarden waaronder de politie de software en systemen heeft afgenomen, of heeft willen afnemen, van de betrokken bedrijven. Dat zijn nog steeds actuele voorwaarden. Zouden deze openbaar worden gemaakt, dan zou dat de onderhandelingspositie van de politie schaden bij toekomstige onderhandelingen over de aanschaf en het onderhoud van vergelijkbare software en/of systemen, wat het goed functioneren van de politie in het algemeen zou schaden.

Het voorgaande brengt met zich mee, dat aan het belang van het goed functioneren van de politie meer gewicht toekomt dan het belang van openbaarheid, zodat deze informatie op grond van artikel 5.1 lid 2 onder i van de Woo niet openbaar kan worden gemaakt.

#### **Artikel 5.1, lid 5 van de Woo (cijfercode 13)**

In uitzonderlijke gevallen kan openbaarmaking (van andere informatie dan milieu-informatie) voorts achterwege blijven indien openbaarmaking onevenredige benadeling toebrengt aan een ander belang dan genoemd in het eerste of tweede lid van artikel 5.1 en het algemeen belang van openbaarheid niet tegen deze benadeling opweegt.

Deze uitzonderingsgrond is toegepast op (digitaal)technische (delen van) teksten oftewel op zogeheten 'padnamen'/'link(s)' naar bestanden/digitale locaties die de politie hanteert. Dit op grond van het feit dat de politie onaanvaardbare (inter)nationale veiligheidsrisico's loopt indien de 'padbeschrijvingen' / 'link(s)' openbaar zou(den) zijn/worden. Gezien de huidige tijd en dus de (vergevoerde) (door)ontwikkelingen van kennis en kunde op het gebied van het hacken van systemen, is het niet ondenkbaar dat kwaadwillenden zullen proberen via deze gegevens in te breken in de (structuur van) politiestructuren. Document met nummer 102 bevat een dergelijke link die verwijst naar een interne digitale locatie van de politie. Om die reden maak ik deze informatie niet openbaar.

### **Algemeen**

Gelet op het bovenstaande, wordt geoordeeld dat in redelijkheid de voornoemde belangen zwaarder dienen te wegen dan het zwaarwegende belang van openbaarmaking en wordt deels overgegaan tot het openbaar maken informatie, waarmee het publieke belang van een goede en democratische bestuursvoering is gewaarborgd.