Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DGOBR - RijksBVA
Ministerie BZK

Datum
24 juli 2014

Kenmerk
2014-0000418177

Protocol uitwisseling van persoonsgerelateerde beveiligingsinformatie

Doel van dit Protocol

1. Het doel van dit protocol is om duidelijkheid te verschaffen over het uitwisselen van persoongerelateerde beveiligingsinformatie binnen het beveiligingsdomein van het Rijk en wie daarvoor verantwoordelijk is[1]. Dit protocol draagt eveneens bij aan een Rijksbreed uniform handelen op dit terrein.
2. Dit protocol is bedoeld voor alle medewerkers die uitvoering geven aan de beveiliging van de te beschermen belangen van het Rijk. Onder 'Rijk' wordt hier verstaan de verzameling organisaties waarop het Beveiligingsvoorschrift Rijksdienst (BVR 2013) van toepassing is.

Uitwisselen van beveiligingsgerelateerde informatie

3. Binnen het Rijk worden fysieke beveiligingsmaatregelen getroffen die gebaseerd zijn op Rijksbrede normenkaders, waaronder het:
    a. Kader Rijkstoegangsbeleid (2010)
    b. Normenkader Beveiliging Rijkskantoren (NkBR 2013)
    c. Voorschrift informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI 2013) .

    Deze beveiligingsmaatregelen en procedures zijn in principe voldoende om onder reguliere omstandigheden beveiligingsrisico's tot een aanvaardbaar niveau te beperken.
4. Desondanks kan het nodig zijn om in bepaalde situaties een extra waarschuwing te versturen naar collega's binnen het beveiligingsdomein van het Rijk, om hen zo te informeren over concrete beveiligingsrisico's en hen in staat te stellen hier tijdig en adequaat op te reageren. Dit kunnen bijvoorbeeld waarschuwingen zijn naar beveiligers van objecten in een bepaald gebied waarin gewezen wordt op mogelijke openbare orde verstoringen die de veiligheid van het kantoor/object of van de medewerkers, nadelig zouden kunnen beïnvloeden.
5. Dergelijke beveiligingsberichten kunnen er ook op gericht zijn om collega's te waarschuwen voor bepaald risicovol gedrag, zoals wanneer personen:
    a. zich dreigend hebben uitgelaten richting medewerkers (inclusief bewindspersonen) van een rijkskantoor/-object.

[1] Het onderhavige protocol bestrijkt alleen het onderwerp informatie uitwisseling. Daarmee kan het een overlap vertonen met bestaande of toekomstige departementale regels of voorzieningen zoals Wbp-meldingen of protocollen. Daarom zal dit protocol deel uitmaken van bestaand, of nog te ontwikkelen beleid, maatregelen en (controle)mechanismen die bedoeld zijn om ervoor te zorgen en te kunnen aantonen dat de verwerking van persoonsgegevens in het beveiligingsdomein in overeenstemming met de Wbp wordt uitgevoerd. Daarnaast past dit protocol binnen de afspraken en kaders zoals vastgelegd in de Circulaire Bewaken en beveiligen van personen, objecten en diensten.

b. zich eerder schuldig hebben gemaakt aan vernieling, diefstal of andere strafbare feiten op, rond of in een rijkskantoor/-object.
c. het functioneren (het ongestoord handelen) van een rijksoverheidsorganisatie al eerder hebben verstoord.

Voor de inhoud van het beveiligingsbericht geldt als uitgangspunt hetgeen onder 6 wordt genoemd. Als sprake is van een concrete en serieus geachte (gewelds) dreiging kan de uitzondering worden gevolgd zoals benoemd onder 7-8.

Uitgangspunt: berichten zijn geanonimiseerd en veralgemeniseerd

6. Ten aanzien van de inhoud van interne beveiligingsberichten gelden de volgende uitgangspunten:
    a. Een waarschuwing is altijd gebaseerd op een concrete melding of informatie. Alvorens een waarschuwingsbericht te versturen dient altijd de bron en juistheid van de gegevens onderzocht en geverifieerd te zijn. In het bericht zelf dient aangegeven te worden wat de bron is van de melding/informatie, door wie de melding is gecheckt en bij welke partij(-en) dat is gebeurd.
    b. Waarschuwingen voor risicovolle gedragingen dienen in beginsel geanonimiseerd en veralgemeniseerd te worden. Dat betekent dat in de waarschuwingen niet de persoonsgegevens van een persoon of personen zijn terug te vinden en dat de waarschuwing voor de risicovolle gedragingen van de betreffende persoon wordt omgevormd tot een algemene waarschuwing voor een bepaald risico. Zo wordt niet gewaarschuwd voor één specifieke fietsendief maar wordt de aandacht gevestigd op het (beter) voorkomen en signaleren van fietsendiefstallen. Ook wordt niet gewaarschuwd voor het gebruik van onjuiste of vervalste identiteitsbewijzen door één persoon maar wordt de aandacht gevestigd op een juiste controle van identiteitsbewijzen.
    c. Dit betekent ook dat de waarschuwingen niet mogen leiden tot een op de persoon gerichte beveiligingsaanpak. De beveiliging mag dus in principe geen andere of extra beveiligingsmaatregelen nemen speciaal gericht op of tegen één of enkele personen.

Uitzondering bij concrete dreiging

7. Op het moment dat een BVA informatie ontvangt (bijvoorbeeld via een schriftelijke bedreiging) waaruit een concrete en serieus geachte dreiging blijkt richting personen of objecten binnen zijn departement, dan kan hij de departementale beveiligingsorganisatie hierover informeren. In beginsel wordt hierbij de onder 6 genoemde werkwijze gehanteerd. Eventueel kunnen ook persoonsgegevens worden verstrekt, voor zover dat noodzakelijk is, om gelet op de aard van de dreiging, een tijdig en adequaat handelen van de beveiligingsorganisaties te verzekeren. Het is de BVA die bepaalt of dit noodzakelijk is. In het geval er persoonsgegevens moeten worden uitgewisseld binnen de departementale beveiligingsorganisatie geldt de volgende werkwijze:
    a. Het uitwisselen van persoonsgegevens dient altijd zoveel mogelijk te worden beperkt, waarbij alleen gegevens mogen worden uitgewisseld die nodig zijn voor een tijdig en adequaat handelen van de beveiligingsorganisaties.
    b. Om een persoon tijdig te kunnen herkennen kan het nodig zijn om foto's van de betreffende persoon aan het bericht toe te voegen. In dat geval geldt dat alleen foto's uit open bronnen mogen worden toegevoegd.
    c. Justitiële gegevens/antecedenten van de betreffende persoon mogen niet worden meegestuurd. Een uitzondering hierop vormen de gegevens over eerdere wetsovertredingen die nodig zijn om een veilig en adequaat handelen van het beveiligingspersoneel te borgen.
    d. De betreffende berichten worden altijd voorzien van de markering 'vertrouwelijk behandelen'.

8. Wanneer de concrete en serieus geachte (gewelds)dreiging uitgaat richting één of meerdere bewindspersonen informeert de BVA, naast het doen van aangifte bij het Team Bedreigde Politici van politie Haaglanden, tevens de NCTV in verband met de uitvoering van het stelsel bewaken en beveiligen. Indien de dreigingsinformatie rechtstreeks bij de NCTV binnenkomt informeert de NCTV de desbetreffende BVA. Zo nodig kan de BVA (delen van) dit bericht conform artikel 6 of 7 a t/m c vervolgens door (laten) zetten binnen de beveiligingsorganisatie van het departement.

Ontvangers

9. Beveiligingsberichten mogen alleen verstuurd worden aan partijen die belast zijn met taken op het gebied van de (fysieke) beveiliging van de Rijksoverheid, én alleen voor zover dat noodzakelijk is voor de uitvoering van hun taak. De verspreiding van persoonsgegevens dient derhalve altijd zo beperkt mogelijk plaats te vinden. Als de dreiging bijvoorbeeld van dien aard is dat het noodzakelijk is om bepaalde persoonsgerelateerde informatie te verstrekken, en deze betrekking heeft op een bepaalde locatie of een bepaald ministerie, dan zal de verspreiding van de informatie beperkt moeten worden tot de beveiliging van één pand of de panden van één ministerie. Het ongericht of onbeperkt versturen van informatie binnen het beveiligingsdomein dient te allen tijde voorkomen te worden.

Werking

10. Dit protocol treedt per 1 augustus 2014 in werking.