Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2483

Vragen van het lid **Schilder** (Groep Markuszower) aan de Staatssecretaris van Justitie en Veiligheid over *een ernstig datalek binnen de EBI* (ingezonden 4 juni 2026).

Antwoord van Staatssecretaris **Van Bruggen** (Justitie en Veiligheid) (ontvangen 6 juli 2026). Zie ook Aanhangsel Handelingen, vergaderjaar 2025–2026, nr. 2378.

Vraag 1
Heeft u kennisgenomen van berichtgeving dat vertrouwelijke dossierinformatie van een gedetineerde met een zware risicostatus zichtbaar is geweest voor een andere gedetineerde binnen de Extra Beveiligde Inrichting (EBI)?[1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u het feit dat juist binnen de zwaarst beveiligde inrichting van Nederland vertrouwelijke strafrechtelijke informatie kennelijk bij een andere gedetineerde terecht heeft kunnen komen?

Antwoord 2
Uit onderzoek naar het incident blijkt dat tijdens het volgen van de procedure sprake is geweest van een menselijke fout. Op basis van het onderzoek valt niet vast te stellen of daadwerkelijk inzage in vertrouwelijke informatie heeft plaatsgevonden. Dit moet echter te allen tijde worden voorkomen. DJI treft dan ook aanvullende maatregelen om de kans op herhaling te verkleinen. Zo is een extra controlestap in de procedure aangebracht die ziet op het uitschakelen van de laptop. Ook voert DJI daarnaast nog enkele technische verbeteringen door. Vanuit een veiligheidsoogpunt kan ik deze niet gedetailleerd delen.

[1] Telegraaf, 3 juni 2026, Blunder: vertrouwelijke informatie Marengo-kopstuk Saïd Razzouki belandt op laptop medegedetineerde (https://www.telegraaf.nl/misdaad/blunder-vertrouwelijke-informatie-marengo-kopstuk-sad-razzouki-belandt-op-laptop-medegedetineerde/155020872.html).

ah-tk-20252026-2483
ISSN 0921 - 7398
's-Gravenhage 2026

Vraag 3
Klopt het dat de voorgeschreven veiligheidsprocedures in dit geval niet zijn gevolgd? Zo ja, hoe heeft dit kunnen gebeuren?

Antwoord 3
Uit onderzoek is gebleken dat tijdens het volgen van deze procedure sprake is geweest van een menselijke fout. DJI treft maatregelen om de kans op herhaling te verkleinen.
De reguliere procedure is dat nadat een gedetineerde een dergelijke laptop heeft gebruikt, de laptop wordt uitgeschakeld. Door middel van het uitschakelen van de laptop wordt alle historie automatisch verwijderd en daarmee «geschoond». Pas daarna mag de laptop worden uitgegeven aan een andere gedetineerde.

Vraag 4
Geeft dit incident aanleiding tot het herzien van de veiligheidsprocedures? Zo nee, waarom niet?

Antwoord 4
De resultaten van het onderzoek naar aanleiding van het incident geven aanleiding tot het treffen van maatregelen. Zoals toegelicht in het antwoord op vraag 1, betreft dit een extra controlestap.

Vraag 5
Kan worden uitgesloten dat vertrouwelijke informatie van andere gedetineerden eveneens onbevoegd is ingezien? Zo nee, waarom niet?

Antwoord 5
Op basis van het onderzoek valt niet vast te stellen of daadwerkelijk inzage in vertrouwelijke informatie van de betreffende gedetineerde heeft plaatsgevonden. Vanwege veiligheidsredenen kan niet verder worden ingegaan op de details van het onderzoek.
Er is nu geen aanleiding te vermoeden dat vergelijkbare incidenten zich eerder hebben voorgedaan.

Vraag 6
Deelt u de mening dat een dergelijke blunder ernstige veiligheidsrisico's met zich kan brengen voor lopende strafzaken, getuigen, slachtoffers, personeel en de openbare veiligheid? Zo nee, waarom niet?

Antwoord 6
Ik wil voorop stellen dat ik het uiteraard betreur dat deze fout zich voor heeft kunnen doen. Zoals aangegeven in mijn vorige antwoord op vraag 5, valt op basis van het onderzoek niet vast te stellen of daadwerkelijke inzage in vertrouwelijke informatie heeft plaatsgevonden.
Het Openbaar Ministerie, de betrokken gedetineerde en diens advocaat zijn inmiddels geïnformeerd. Het onderzoek heeft in afstemming met hen plaatsgevonden. Bij het vermoeden van een datalek is vereist dat binnen 72 uur een melding hiervan wordt gedaan bij de Autoriteit Persoonsgegevens. DJI heeft dit gedaan. Door DJI wordt op basis van de onderzoeksresultaten bekeken of hier nog verdere actie op moet volgen.

Vraag 7 en 8
Acht u het verantwoord dat gedetineerden met een zware risicostatus zonder toezicht toegang hebben tot apparatuur waarmee dergelijke fouten kennelijk kunnen ontstaan? Zo ja, waarom?
Bent u bereid te onderzoeken of dossierinzage voor hoogrisicogedetineerden voortaan uitsluitend onder toezicht en op papier dient plaats te vinden, zodat deze gedetineerden in zijn geheel geen toegang meer hebben tot laptops, waar wij al eerder voor hebben gepleit, en dit soort datalekken daardoor onmogelijk wordt? Zo nee, waarom niet?

Antwoord 7 en 8
De laptops die aan gedetineerden worden uitgereikt betreffen *stand alone* laptops die uitsluitend over functionaliteiten beschikken om het strafdossier te raadplegen.

Op basis van een uitspraak van RSJ[2] moeten OM en DJI bij omvangrijke dossiers digitale inzage faciliteren. Bovendien is het uitsluitend op papier verstrekken van het strafdossier bij omvangrijke dossiers niet uitvoerbaar vanwege de beheersingsproblematiek die daarbij komt kijken. Niet enkel op het gebied van logistiek (het veilig transporteren van dossier van OM naar gedetineerde, bij overplaatsingen en bij beëindiging van inzage) maar ook op het gebied van informatieveiligheid en fysieke veiligheid (denk aan brandlast op cel).

Vraag 9
Welke disciplinaire, organisatorische of personele consequenties worden verbonden aan het niet naleven van de veiligheidsprocedures die tot dit incident hebben geleid? Gaat de toedracht van dit incident worden onderzocht op mogelijk opzettelijk handelen?

Antwoord 9
Ik ga niet in op individuele personele en disciplinaire kwesties.

Vraag 10
Kunt u garanderen dat zich binnen de EBI momenteel geen vergelijkbare beveiligingslekken voordoen waardoor gedetineerden toegang kunnen krijgen tot informatie die niet voor hen bestemd is? Zo nee, waarom niet?

Antwoord 10
DJI zet zich onvermoeibaar in voor een veilige omgeving, zowel fysiek als digitaal. De extra maatregelen die worden genomen naar aanleiding van het onderzoek zullen hieraan bijdragen.

[2] RSJ 08/2031/GA, 29 januari 2009.