AH 2774

2026Z15519

Antwoord van minister Heerma (Binnenlandse Zaken en Koninkrijksrelaties) en de minister van Defensie (ontvangen 26 augustus 2026)

1. Bent u bekend met het bericht dat de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) heeft geoordeeld dat de AIVD en MIVD niet zorgvuldig zijn omgegaan met verzamelde persoonsgegevens? (Kamerstuk 36263, nr. 50)

Antwoord op vraag 1

Ja.

2. Onderschrijft u dat juist van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD), gelet op de aard en gevoeligheid van de gegevens die zij verwerken, mag worden verwacht dat zij de wettelijke waarborgen voor gegevensverwerking strikt naleven? Zo nee, waarom niet?

Antwoord op vraag 2

Zoals benoemd door de CTIVD, zijn bulkdatasets van groot belang voor de goede taakuitvoering van de wettelijke taken van de diensten. Tegelijkertijd is duidelijk dat het gebruik van bulkdatasets een aanzienlijke privacyinbreuk kan meebrengen. Wij onderschrijven vanzelfsprekend de noodzaak van het bestaan van voldoende waarborgen rondom de verwerking van bulkdatasets, alsook een zorgvuldige implementatie en naleving daarvan. In het algemeen geldt dat deze waarborgen worden nageleefd, maar, zoals de CTIVD heeft geconstateerd, valt er winst te behalen in de uitvoering en (technische) implementatie van die waarborgen. Wij onderschrijven deze constatering. Het verbeteren van het beheer van bulkdatasets staat hoog op de agenda van de diensten. Voorafgaand aan en tijdens de uitvoering van het CTIVD-onderzoek hebben de diensten reeds diverse verbetermaatregelen genomen om tegemoet te komen aan de geconstateerde knelpunten (zie het gebundelde antwoord op vraag 4, 5, 8 en 15). De komende tijd zetten de diensten de implementatie van deze verbetermaatregelen voort. In aanloop naar het nieuwe wetsvoorstel van de Wiv 202X zullen wij daarnaast ook nadrukkelijk aandacht vragen voor de geconstateerde knelpunten rondom de verwerking van bulkdatasets.

3. Welke concrete tekortkomingen heeft de CTIVD vastgesteld in de wijze waarop de AIVD en MIVD persoonsgegevens verwerken, bewaren en toegankelijk maken?

Antwoord op vraag 3

Een groot deel van de bevindingen en aanbevelingen van de CTIVD is te herleiden naar tekortkomingen in het technisch beheer van bulkdatasets, het bijbehorend datamanagement en de (interne) controle op wie toegang heeft (gehad) tot welke data. Voor het volledige overzicht van de bevindingen en aanbevelingen verwijzen wij u naar het rapport van de CTIVD.

4. Hoe heeft het kunnen gebeuren dat deze tekortkomingen zijn ontstaan, terwijl de diensten beschikken over uitgebreide interne controlemechanismen en extern toezicht?

5. Zijn de geconstateerde tekortkomingen het gevolg van onvoldoende capaciteit, onvoldoende deskundigheid, tekortschietende sturing of een andere oorzaak? Kunt u dit toelichten? 8. Welke organisatorische en technische maatregelen zijn inmiddels getroffen om ervoor te zorgen dat wettelijke waarborgen, waaronder autorisatiebeheer, bewaartermijnen en interne controles, structureel worden nageleefd?

15. Welke lessen trekt u uit deze bevindingen om te voorkomen dat vergelijkbare tekortkomingen zich in de toekomst opnieuw voordoen?

Antwoord op vragen 4, 5, 8 en 15 Wij constateren dat zowel de versnippering van het datalandschap als van het stelsel van waarborgen voor de verwerking van bulkdatasets, mede gelet op de administratieve druk die dit met zich meebrengt, het risico op menselijke fouten vergroot. Voorafgaand aan en tijdens de uitvoering van het onderzoek hebben de diensten zelfstandig verschillende risico’s en kwetsbaarheden geïdentificeerd ten aanzien van (de verwerking van) bulkdatasets. In verschillende gevallen hebben deze risico’s daadwerkelijk geleid tot compliance-incidenten, die voorafgaand aan en tijdens het onderzoek aan de CTIVD zijn gemeld. Naar aanleiding van deze incidenten hebben de diensten direct maatregelen getroffen om dergelijke incidenten te detecteren, mitigeren en in de toekomst te voorkomen, dan wel het risico dat dit soort incidenten zich voordoen aanzienlijk te verkleinen. Het betreft hier maatregelen op het gebied van autorisatiebeheer en toegangsmanagement, alsook maatregelen die zien op het vergroten van het bewustzijn bij medewerkers rondom het belang van compliant werken. De eerste belangrijke stappen zijn zodoende al gezet. Tegelijkertijd is duidelijk dat structurele maatregelen nodig zijn. In dat kader verwelkomen wij de bevindingen van de CTIVD, die de urgentie van het onderwerp onderstrepen en oplossingsrichtingen aandragen voor de toekomst waar de diensten vanzelfsprekend voortvarend aan blijven werken. Zoals reeds genoemd is een groot deel van de bevindingen en aanbevelingen van de CTIVD te herleiden naar tekortkomingen in het technisch beheer van bulkdatasets, het bijbehorend datamanagement en de (interne) controle op wie toegang heeft (gehad) tot welke data. Met een aantal van de aanbevelingen uit het rapport zijn de diensten al aan de slag gegaan. Zo werken de diensten aan een applicatie voor toestemmingsverzoeken, waarmee de mogelijkheid om gegevens te raadplegen op geautomatiseerde wijze wordt gekoppeld aan de looptijd van het toestemmingsverzoek en de bijbehorende autorisaties. Daarnaast zullen de AIVD en de MIVD de interne logging van systemen uitbreiden om incidenten waarin autorisatiebeheer een rol speelt in de

toekomst zo veel mogelijk te kunnen voorkomen, sneller te kunnen detecteren en beter te kunnen mitigeren. Dit draagt bij aan compliant werken. Wij onderstrepen evenwel dat de benodigde technische verbetermaatregelen aanpassingen vergen, bijvoorbeeld in de IT-systemen, die tijd en capaciteit kosten. De realisatie van deze structurele verbeteringen zal daarom een substantiële en consistente inspanning vergen. De diensten zullen de CTIVD periodiek op de hoogte houden van de ontwikkelingen en vorderingen op dit gebied.

Tot slot, zullen wij in aanloop naar het nieuwe wetsvoorstel van de Wiv 202X ook nadrukkelijk aandacht vragen voor de geconstateerde knelpunten rondom de verwerking van bulkdatasets.

6. Heeft de CTIVD eerder vergelijkbare tekortkomingen gesignaleerd? Zo ja, welke aanbevelingen zijn destijds gedaan en waarom hebben deze kennelijk niet voorkomen dat de huidige situatie is ontstaan?

9. Wanneer zijn de geconstateerde tekortkomingen voor het eerst ontstaan en sinds wanneer was u hiervan op de hoogte?

Antwoord op vragen 6 en 9

De CTIVD heeft eerder vergelijkbare tekortkomingen gesignaleerd. In toezichtrapporten nr. 70 en 71 over de verwerking van passagiersgegevens van luchtvaartmaatschappijen en het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan heeft de CTIVD ook aandacht gevraagd voor de naleving van de waarborgen voor de verdere verwerking van bulkdatasets. Naar aanleiding van deze rapporten hebben onze ambtsvoorgangers de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 geïntroduceerd, met daarin aanvullende waarborgen en maatregelen die meer recht doen aan de bescherming van fundamentele rechten van burgers en de operationele waarde van bulkdatasets voor de diensten. De CTIVD stelt nu vast dat in de uitvoering en (technische) implementatie van die waarborgen nog winst valt te behalen. Wij herkennen ons in dat beeld en zetten het reeds ingezette verbetertraject de komende tijd voort (zie het antwoord op vraag 4-5-8-15).

7. Is naar uw oordeel sprake van tekortschietende uitvoering van bestaande wettelijke regels, of acht u de huidige wettelijke kaders onvoldoende duidelijk, vaag, uitvoerbaar of te strict? Kunt u uw antwoord toelichten?

Antwoord op vraag 7 De Wiv 2017 kent geen speciale regels voor het gebruik van bulkgegevens, met uitzondering van de bulkgegevens die worden verzameld met de inzet van onderzoeksopdrachtgerichte (OOG) interceptie. In de praktijk heeft dat geleid tot onduidelijkheden en een onoverzichtelijk stelsel voor de verdere verwerking van bulkgegevens. Mede naar aanleiding van toezichtrapporten van de CTIVD is de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 opgesteld. De CTIVD heeft geconstateerd dat het huidig wettelijk kader in beginsel voldoende waarborgen biedt, maar dat winst te behalen valt in de uitvoering en (technische) implementatie van deze waarborgen. Wij onderschrijven deze constatering. Tegelijkertijd stellen wij vast dat zowel de versnippering van het datalandschap als van het stelsel

van waarborgen voor de verwerking van bulkdatasets, mede gelet op de administratieve druk die dit meebrengt, het risico op menselijke fouten vergroot. In aanloop naar het nieuwe wetsvoorstel van de Wiv 202X zullen wij nadrukkelijk aandacht vragen voor deze en andere geconstateerde knelpunten rondom de verwerking van bulkdatasets.

10. Hoe wordt periodiek gecontroleerd of deze maatregelen daadwerkelijk functioneren en hoe wordt de Kamer hierover geïnformeerd, voor zover de staatsveiligheid zich daar niet tegen verzet?

Antwoord op vraag 10

De diensten hebben sinds april 2023 een compliance-meldingssysteem. Dit wordt doorlopend geprofessionaliseerd. Daarnaast wordt er hard gewerkt aan het vergroten van het compliance-bewustzijn binnen de diensten om compliance incidenten zoveel mogelijk te voorkomen en daar waar onverhoopt toch iets misgaat deze incidenten vroegtijdig te detecteren en te mitigeren. Met de CTIVD is in 2023 overeengekomen dat naast het systeemtoezicht van de CTIVD, door de diensten een intern compliance-managementsysteem zou worden ingericht, waar een intern inschalingsmodel voor compliance-incidenten deel van uitmaakt. De diensten en de CTIVD hebben hiervoor gezamenlijk een incidentenprotocol opgesteld waarin is opgenomen hoe moet worden omgegaan met compliance-incidenten en wie wanneer daarover geïnformeerd dient te worden. De CTIVD houdt regulier toezicht op het compliance-meldingssysteem en kan hierover, indien aangewezen, rapporteren. Het ligt niet voor de hand, gelet op het efficiënt functioneren van het interne compliance-managementsysteem, dat wij uw Kamer, anders dan via de openbare jaarverslagen of de daarvoor geëigende kanalen, informeren over compliance-incidenten.

11. Wordt bij de ontwikkeling of aanbesteding van nieuwe informatiesystemen standaard getoetst of wettelijke bewaartermijnen, autorisaties en logging automatisch worden afgedwongen?

Antwoord op vraag 11

Gezien de specifieke aard van onze werkzaamheden worden veel informatiesystemen in het operationele domein door de diensten zelf ontwikkeld. Hierbij worden wettelijke vereisten zoals bewaartermijnen en autorisaties en functionele eisen zoals logging, integraal onderdeel gemaakt van het ontwikkelproces. Autorisatiebeheer en logging zijn essentieel voor de operationele veiligheid, betrouwbaarheid, beschikbaarheid en vertrouwelijkheid van de data van de diensten. Deze vormen derhalve vanzelfsprekend een belangrijke leidraad bij de ontwikkeling van nieuwe informatiesystemen.

12. Bent u van oordeel dat de huidige systemen van de AIVD en MIVD zodanig zijn ingericht dat wettelijke waarborgen technisch worden afgedwongen ("security by design" en "privacy by design")? Zo nee, waarom niet?

Antwoord op vraag 12

Hoewel niet alle waarborgen volledig technisch te automatiseren zijn, zijn er adequate controles aanwezig om de naleving ervan te waarborgen. Het

waarborgen van security - en privacy by design is een continu proces van optimalisatie en onderdeel van de ICT-architectuur. De aanbevelingen uit het CTIVD-rapport worden gebruikt voor de verdere aanscherping van processen en ICT-architectuur. Daarnaast biedt de in voorbereiding zijnde nieuwe Wiv 202X, waarvan de contouren reeds zijn geschetst, een verbeterd en essentieel kader om de ondersteuning van het inlichtingenproces op het gebied van rechtmatigheid en technische borging verder te professionaliseren en te optimaliseren waarbij tegelijkertijd geen afbreuk wordt gedaan aan de operationele slagkracht van beide diensten.

13. Kunt u uitsluiten dat vergelijkbare tekortkomingen zich ook voordoen bij andere overheidsorganisaties die grote hoeveelheden gevoelige persoonsgegevens verwerken? Zo nee, bent u bereid hiernaar onderzoek te laten verrichten?

Antwoord op vraag 13

Het verzamelen van bulkinformatie is uniek voor de AIVD en de MIVD. Als hiervoor verantwoordelijke ministers informeren we u in deze antwoorden hoe we het beheer van deze bulkdatasets de komende tijd verder gaan versterken. In algemene zin doen alle overheidsinstanties altijd hun best om persoonsgegevens die onder hun verantwoordelijkheid vallen zo goed mogelijk te beheren. Dat zich daarbij tekortkomingen kunnen voordoen, kan helaas nooit helemaal worden uitgesloten. Ook daar zijn toezichthoudende instanties die daar op permanente basis onderzoek naar doen. In voorkomend geval kan de verantwoordelijke minister besluiten tot een aanvullend onderzoek.

14. Deelt u de opvatting dat de bescherming van gevoelige persoonsgegevens in de eerste plaats afhankelijk is van een zorgvuldige uitvoering van wettelijke waarborgen, goed ingerichte processen en deugdelijk toezicht, ongeacht de herkomst van de gebruikte technologie of leveranciers? Zo nee, waarom niet?

Antwoord op vraag 14

Wij onderschrijven de noodzaak van het hebben van voldoende waarborgen en een zorgvuldige implementatie en naleving daarvan, ongeacht technologie of leverancier. Deze waarborgen zijn nodig om recht te doen aan de bescherming van de fundamentele rechten van burgers.

16. Kunt u de vragen afzonderlijk beantwoorden?

Antwoord op vraag 16 Vraag 6 en 9 en 4, 5, 8,en 15 zijn gezamenlijk beantwoord. De overige vragen zijn separaat beantwoord.