Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 789 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 oktober 2021

Op 16 juli jl. (Kamerstukken 26 643 en 32 761, nr. 775) heb ik uw Kamer geïnformeerd over een datalek binnen mijn ministerie. Dit betrof persoonsgegevens van een groot aantal medewerkers van JenV-organisaties en een kleiner aantal medewerkers van andere organisaties. Het datalek was veroorzaakt door een voormalige externe medewerker bij mijn ministerie die -tegen de regels in- een bestand van JenV naar een eigen werkomgeving had gekopieerd en vervolgens naar twee andere overheidsorganisaties, waarvoor hij opdrachten uitvoerde.

Na de constatering van het datalek is direct een melding gedaan bij de Autoriteit Persoonsgegevens (AP) en heb ik opdracht gegeven voor een drietal onderzoeken naar de oorzaak en impact van het datalek. In deze brief ga ik in op de uitkomsten van deze onderzoeken en de door mij (op basis daarvan) getroffen maatregelen.

Uitgevoerde onderzoeken

De volgende drie onderzoeken zijn uitgevoerd:
- Het Integriteitsbureau DJI verrichtte onderzoek naar het feitelijke handelen van de externe medewerker en zijn interne collega's.
- Het bedrijf Fox-IT verrichtte forensisch onderzoek naar welke personen en/of organisaties mogelijk toegang hebben of hadden tot het gegevensbestand.
- De Auditdienst Rijk (ADR) verrichtte een onderzoek naar het gebruik en beheer van de betrokken (identiteits-)gegevens binnen JenV, de daarbinnen getroffen maatregelen, de navolging daarvan in relatie tot het incident en mogelijke verbetermaatregelen.

Onderzoeksuitkomsten

Voor het integriteitsonderzoek hoorde het onafhankelijke integriteitsbureau de externe medewerker en een aantal interne medewerkers. Hieruit is gebleken dat de externe medewerker zonder medeweten van

kst-26643-789
ISSN 0921 - 7371
's-Gravenhage 2021

zijn interne collega's bij het Bestuursdepartement van JenV of het Openbaar Ministerie (OM) de data naar de andere werkomgevingen bracht. De externe medewerker kende de geldende gedragsregels en handelde daarmee in strijd. Op een aantal punten hadden de werkafspraken over de voorwaarden waaronder hij de persoonsgegevens waar hij toegang toe had verder mocht verwerken met de externe medewerker scherper kunnen worden gemaakt en vastgelegd. En tenslotte was de externe medewerker ten aanzien van het transporteren van de data zich naar eigen zeggen niet bewust dat zijn handelen betekende dat er een datalek ontstond.

Het onderzoek van Fox-IT bevestigt dat de data buiten JenV aanwezig is geweest bij het OM, de GGD-GHOR en de werkgever van de betrokken externe medewerker, en inherent daaraan bij de IT-dienstverleners van deze organisaties. Daarnaast heeft het onderzoeksbureau dat het gegevenslek heeft ontdekt bij de GGD-GHOR toegang gehad tot de data. Fox-IT heeft geen aanwijzingen gevonden die erop duiden dat het bestand op andere locaties was (of is) opgeslagen en door onbevoegden is ingezien of gebruikt, hoewel dit door de beperkte beschikbaarheid van logbestanden niet met volledige zekerheid kan worden uitgesloten.

Het ADR-onderzoek toont aan dat bij de betrokken afdeling van het Ministerie van JenV de noodzakelijke waarborgen omtrent geheimhouding, privacybescherming en integriteit zijn ingericht en dat ook regelmatig een evaluatie plaatsvindt van de beheer- en werkprocessen. Wel benoemt het onderzoek mogelijkheden voor verbetering in de *naleving* van de procedurele en administratieve waarborgen. Ook benoemt het onderzoek dat aan het gebruik van de MS Access tool risico's zijn verbonden die in eerder uitgevoerde risicoanalyses niet waren onderkend, bijvoorbeeld op het gebied van toegangsbescherming. Het rapport geeft adviezen voor aanscherping en verbetering van een aantal procedures/regels en over de gebruikte analysetool.

Opvolging

Er zijn geen aanwijzingen dat het bestand op andere locaties aanwezig was (of is) dan de al genoemde organisaties. Daarom verandert de eerder vastgestelde reikwijdte van het datalek niet en is de eerder gedane melding aan de AP afgesloten.

Ik constateer op basis van de onderzoeksuitkomsten dat het datalek het gevolg is van het individuele handelen van de externe medewerker en niet van ernstige tekortkomingen in de werkwijze bij de verwerking van de betrokken persoonsgegevens. Binnen mijn ministerie wordt lering getrokken uit dit incident en wordt opvolging gegeven aan de verbeteradviezen van de ADR. De werkafspraken en procedures bij inhuur van medewerkers en het databeheer binnen de betrokken afdeling worden aangescherpt. Er wordt scherper gekeken naar dataminimalisatie («voor welk doel is welke informatie echt nodig»). Daarnaast is er een project gestart om de betreffende analysetool te vervangen en op termijn staat de invoering van Data Leakage Protection (DLP) gepland. DLP is tooling om vertrouwelijke en niet-gerubriceerde informatie te onderscheiden en bijvoorbeeld het transporteren daarvan te signaleren. Verder zal het bewustzijn van beveiligingsrisico's en de kennis van veilig digitaal werken van medewerkers die vergaande toegang hebben tot gegevens worden vergroot door het bewustwordingsprogramma «Weerbaar JenV».

Het geheel overziend en de resultaten van de onderzoeken afwegend heb ik besloten vooralsnog geen aangifte te doen. Ik heb de externe medewerker, diens werkgever en de mantelpartij via welke betrokkene

was ingehuurd wel aansprakelijk gesteld voor de door de Staat geleden of te lijden schade.

Communicatie

De in het datalek betrokken personen en organisaties zijn geïnformeerd over de uitkomsten van de onderzoeken en de door mij genomen maatregelen. De veiligheid van de persoonsgegevens van de medewerkers van de Rijksdienst dient te allen tijde geborgd te worden. Ik betreur het incident en zet met het opvolgen van de verbeteradviezen in op een nog betere bestendiging van dit veiligheidsaspect.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus