Ontvangstbevestiging

Uw verzoek tot het indienen van een melding wordt in behandeling genomen.
U kunt de melding niet online raadplegen. Maak daarom een print voor uw eigen administratie. Doe dit voordat u deze pagina afsluit. Na het afsluiten van deze pagina zijn de gegevens die u heeft opgegeven niet meer beschikbaar. Onder het onderstaande meldingsnummer is de melding bekend bij de Autoriteit Persoonsgegevens. U heeft het meldingsnummer nodig om de melding aan te kunnen passen of in te kunnen trekken. Vermeld het meldingsnummer bij eventuele correspondentie met de Autoriteit Persoonsgegevens over de melding.

Tijdstip ontvangst	20-08-2020 13:51:37
Uniek nummer	68efcd33-5e71-4230-9be6-bedf3bd2834b

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?	Een nieuwe melding indienen
Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1. Contactgegevens en overige algemene informatie

1.1 Contactgegevens

Over welke organisatie of welk bedrijf gaat het?

Naam van het bedrijf of de organisatie	Ministerie van Defensie
Adres	Kalvermarkt 32
Postcode	2511CK
Plaats	Den Haag
In welke sector is de organisatie of het bedrijf actief?	Openbaar bestuur - Rijksoverheid

Wie meldt het datalek?

Naam	[redacted]
Functie	AVG Coordinator

E-mailadres	
Telefoonnummer	

Met wie kan de Autoriteit Persoonsgegevens contact opnemen voor nadere informatie over de melding?

De melder is contactpersoon	Ja

1.2 Betrokkenheid andere organisatie

Was er een andere organisatie betrokken bij de inbreuk?	Nee

2. Tijdlijn

Startdatum van de periode waarbinnen de inbreuk was	26-11-2010
Einddatum van de periode waarbinnen de inbreuk was	26-11-2010
Duurt de inbreuk op dit moment nog voort?	Ja
Wanneer werd de inbreuk ontdekt?	29-07-2020
Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?	De Landsadvocaat heeft op maandag 17 augustus jl. geadviseerd om het datalek volledigheidshalve te melden bij de AP.

3. Gegevens over het datalek

3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens	Nee
Inbreuk op de integriteit van de gegevens	Nee
Inbreuk op de beschikbaarheid van de gegevens	Ja

3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?	Overig

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van

persoonsgegevens is geweest

Vastgesteld is dat de logs over de aangeven periode in 2010 van het Geneeskundig Informatiesysteem Defensie (GIDS) ontbreken. Deze logs bevatten informatie over welke artsen wie wanneer welk medisch dossier heeft ingezien. Het ontbreken van de logs is aan het licht gekomen naar aanleiding van een inzageverzoek van een betrokkene in zijn medisch dossier. Betrokkene heeft Defensie hierop gewezen. Uit onderzoek bleek op 29 juli 2020 dat de ontbrekende log als verloren moeten worden beschouwd, het betreft de (externe) loggingsgegevens waarmee wordt bijgehouden wie op welk moment toegang heeft gehad tot het medisch dossier. Er zijn geen aanwijzingen dat gedurende deze periode de inhoud van de medische dossiers is aangetast. Ook de inhoud van het medisch dossier is intact gebleven en de interne logging die plaatsvindt binnen het dossier – oftewel de logging binnen het medisch dossier waaruit volgt welke data aan een medisch dossier is toegevoegd, gewijzigd of verwijderd door een bevoegde zorgverlener – is nog steeds beschikbaar. Ten aanzien van het onderzoek is gebleken dat de logs in deze periode vermoedelijk bij een systeemmigratie in het weekend van 4 maart 2011 abusievelijk niet zijn meegenomen. Het ontbreken van de logs is (ondanks gebruikers- en acceptatietesten) destijds niet opgemerkt. Er is gebleken dat er evenmin back-ups bestaan van de ontbrekende logs. Hoewel voorafgaand en na de systeemmigratie conform geldende procedures back-ups gemaakt van alle bestanden, zijn deze back-up bestanden overeenkomstig de gebruikelijke bewaartermijn van 28 dagen vernietigd. De logs zijn daardoor niet meer beschikbaar.

4. Persoonsgegevens die betrokken zijn bij het datalek

4.1 Persoonsgegevens in het algemeen

Naam	Nee
Geslacht, geboortedatum en/of leeftijd	Nee
Burgerservicenummer (BSN)	Nee
Contactgegevens	Nee
Toegangs- of identificatiegegevens	Ja
Financiële gegevens	Nee
(Kopieën van) paspoorten of andere legitimatiebewijzen	Nee
Locatiegegevens	Nee
Persoonsgegevens betreffende	Nee

strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen	
Onbekend / anders, namelijk:	Loggingsbestand

4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt	Nee
Persoonsgegevens waaruit iemands politieke opvattingen blijken	Nee
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken	Nee
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt	Nee
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid	Nee
Gegevens over iemands gezondheid	Nee
Genetische gegevens	Nee
Biometrische gegevens	Nee

4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk	700000

5. De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers	Ja
Klanten (huidig en potentieel)	Nee
Leerlingen of studenten	Nee
Patiënten	Ja
Minderjarigen	Nee
Personen uit kwetsbare groepen	Nee

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Personen met een medisch dossier bij Defensie

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	5000
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?	14000

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?	Nee

7. Gevolgen van het datalek

7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens	Nee
De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt	Nee
Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt	Nee
Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties	Nee
Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen	Nee
Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen	Nee

7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie	Nee
Identiteitsdiefstal of -fraude	Nee
Financiële verliezen	Nee
Reputatieschade	Nee
Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens	Nee
Ongeoorloofde ongedaanmaking van pseudonimisering	Nee
Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen	Ja
Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen	Ja
Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen	2. Beperkt

8. Vervolgacties naar aanleiding van het datalek

8.1 Informeren van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?	Nee
Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?	0
Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?	geen
Waarom ziet u af van het melden van het datalek aan de betrokkenen?	Anders, namelijk:

Welke andere redenen heeft u om de betrokkenen niet te informeren?

De inhoud van de medische dossier is nog steeds beschikbaar. De ernst van het risico is beperkt, het betreft logs van de periode 16 april 2010 tot en met 26 november 2010. De logging van de handelingen binnen het medisch dossier in de desbetreffende periode nog steeds beschikbaar zijn.

8.2 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?
In de generieke selectielijst Defensie wordt de bewaar-/vernietigingstermijn van de (externe) logbestanden expliciet gemaakt.

8.3 Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking, en is de AP voor deze verwerking de leidende toezichthouder?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?	Nee
Heeft uw organisatie of bedrijf, het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?	Nee

9. Overig

Is naar uw mening deze melding compleet?	Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig