Ontvangstbevestiging van melding inbreuk

Dit is de kopie van uw melding van een inbreuk aan de Autoriteit Persoonsgegevens ten behoeve van uw eigen administratie.

Bewaar deze kopie goed. Bij twijfel kunt u met deze kopie achteraf aantonen dat u een melding van een inbreuk heeft gedaan bij de AP.

Meldingsnummer: 5.1.1e

Melddatum: 25 juli 2025

Meldtijdstip: 11:55

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?	Een nieuwe melding doen van een inbreuk
Wat voor soort datalekmelding wilt u doen?	Ik wil één inbreuk melden (reguliere melding)

1.2 Meldplicht AVG, Tw, Wjsg of Wpg

Op grond van welke wettelijke bepaling doet u deze melding?	Algemene verordening gegevensbescherming (AVG)

1.3 Andere toezichthouders

Heeft uw organisatie of bedrijf de inbreuk gemeld bij toezichthouders op andere meldplichten? Of gaat u dat nog doen?	Nee

2 Internationale aspecten

2.1 Grensoverschrijdende inbreuk

Heeft de inbreuk gevolgen voor personen in meerdere landen?	Nee

3 De verwerkingsverantwoordelijke

3.1 Gegevens verwerkingsverantwoordelijke

Registratienummer van de FG (indien van toepassing)	5.1.1e
KvK-nummer	85036536
Naam van het bedrijf of de organisatie	Justitiële ICT Organisatie
Adres	Stavorenweg 3
Postcode	2803 PT
Plaats	Gouda

In welke sector is de organisatie of het bedrijf actief?

[✓] Openbaar bestuur

[✓] Rijksoverheid

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam	5.1.2e 5.1.2e
Functie	5.1.2e
E-mailadres	5.1.2e @jio.nl
Telefoonnummer	5.1.2e
Tweede telefoonnummer	5.1.2e
Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?	Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?	Ja



4 Tijdlijn

4.1 Duurt de inbreuk op dit moment nog voort?	Onbekend
(Mogelijke) startdatum van de inbreuk	26-5-2025
4.2 Wanneer is het incident ontdekt?	17-7-2025
4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt	De inbreuk is ondekt naar aanleiding van een melding vanuit het NCSC.
Is het moment waarop u het incident heeft ontdekt ook het moment waarop u het incident heeft bestempeld als inbreuk (“datalek”) en dus kennis heeft gekregen van de inbreuk?	Nee
Wanneer heeft u kennis gekregen van het datalek?	24-7-2025

5 Gegevens over de inbreuk

5.1 Aard van de inbreuk

[✓] Persoonsgegevens (mogelijk) ingezien door onbevoegden

5.2 Aard van het incident

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

[✓] Hacking, malware (bijv. ransomware) en/of phishing

Meerdere opties zijn mogelijk binnen het gearceerde deel.

[✓] Ander type hacking en/of malware

Heeft u (digitaal forensisch) onderzoek uitgevoerd of laten uitvoeren naar de aard en de omvang van het datalek?	Ja, het onderzoek loopt

5.3 Beschrijving van het incident

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest	Via een kwetsbaarheid in de Citrix Netscaler heeft een onbekende aanvaller zich toegang verschaft tot een voorportaal van onze digitale werkplek omgeving. Het voorportaal is belangrijk om gebruikers toegang te geven tot de kantoorautomatisering. We hebben als organisatie nauw contact met onze FG en inmiddels worden we ondersteund door medewerkers van de AP.

5.4 Optioneel: upload hier relevante ondersteunende documentatie bij uw melding.

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

[✓] Toegangs- of identificatiegegevens

[✓] Anders

Namelijk:	sessietokens

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

6.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords (persoonsgegevensregisters; artikel 33, lid 3, sub a AVG) zijn getroffen door de inbreuk	1
Geef een toelichting op bovengenoemd aantal:	Het is voor nu onduidelijk om hoeveel gegevensrecords het gaat, dit wordt nog onderzocht.

7 Getroffen personen

7.1 Welke groep(en) betrokkenen is (zijn) getroffen door de inbreuk?

Meerdere opties zijn mogelijk.

[✓] Werknemers

[✓] Anders

Namelijk:	medewerkers van opdrachtgevers
7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.	Medewerkers van JIO en haar opdrachtgevers die afstand hebben ingelogd binnen Citrix.
7.3 Is het exacte aantal betrokkenen bekend?	Nee
Het minimum aantal betrokkenen is:	1
Het maximum aantal betrokkenen is:	1,000

8 Maatregelen vooraf

8.1 Waren de persoonsgegevens voordat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?

[✓] Nee

9 Gevolgen

9.1 (Mogelijke) gevolgen voor de verwerkingsverantwoordelijke en de persoonsgegevens.

Meerdere opties zijn mogelijk.

[✓] Onbevoegden hebben kennis kunnen nemen van de gegevens

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Anders

Namelijk:	Dit is nog onbekend wordt onderzocht.

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)	Aanzienlijk
Licht uw keuze toe:	De onbekende aanvaller zich toegang verschaft tot een voorportaal van onze digitale werkplek omgeving. Het is (nog) niet duidelijk of ze toegang hebben tot onze digitale werkomgeving. Als blijkt dat ze toegang hebben gekregen tot de digitale werkomgeving zijn de gevolgen aanzienlijk.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?	Ja
Aan hoeveel personen heeft u de inbreuk gemeld?	6
Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?	18-7-2025
Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld:	We hebben de inbreuk gemeld aan onze opdrachtgevers. Elke dag wordt er online een status-update gegeven aan de opdrachtgevers.
Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?	Wat er is gebeurd, wat de gevolgen zijn, wat de status is van het onderzoek, welke maatregelen we aan het nemen zijn.

Optioneel: upload hier een kopie van de tekst van deze kennisgeving.

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkene(n) te informeren?

Meerdere opties zijn mogelijk.

[✓] Telefonisch

[✓] Per e-mail

[✓] Via een mededeling op de website

[✓] Anders

Namelijk:	webex

10.2 Motivering niet (persoonlijk) informeren van de betrokkene(n)

Waarom ziet u er van af om (een deel van) de personen van wie gegevens zijn getroffen door de inbreuk te informeren over het incident?

Meerdere opties zijn mogelijk.

[✓] Andere reden(en)

Namelijk:	We zitten nog in de onderzoeksfase

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?	Ja, namelijk:
Toelichting:	Patch doorgevoerd, wachtwoord resets, monitoring uitgebreid.
Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?	Ja, namelijk:
Toelichting:	Monitoring uitgebreid.

11 Verzenden

Op basis van sommige antwoorden die eerder zijn ingevuld in dit meldingsformulier is een vervolgmelding verplicht.

Is dit een voorlopige of een definitieve melding?	Nee, de melding is voorlopig. Er komt later een vervolgmelding met aanvullende informatie over de inbreuk

U bent verplicht een vervolgmelding te doen, omdat mogelijk sprake is van de volgende situatie(s):

- U weet nog niet of u de betrokkene(n) gaat infomeren.
- U heeft aangegeven dat het (digitaal forensisch) onderzoek naar aanleiding van een hacking en/of ransomware incident naar de aard en de omvang van de inbreuk loopt of nog niet is gestart.
- U heeft aangegeven dat u nog niet weet welke persoonsgegevens precies getroffen zijn door de inbreuk.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om de inbreuk te beëindigen.
- U heeft aangegeven nog niet te weten welke maatregelen u heeft getroffen om nieuwe soortgelijke inbreuken te voorkomen.

Geef aan wanneer u (uiterlijk) een vervolgmelding doet	29-8-2025
Toelichting	We verwachten dan meer onderzoeksresultaten te hebben en deze met jullie te kunnen delen.

[✓] Door dit vakje aan te vinken verklaart u dit formulier naar waarheid in te vullen

[✓] Door dit vakje aan te vinken verklaart u bevoegd te zijn deze melding te doen namens uw organisatie.

Privacyverklaring

[✓] Ik ben op de hoogte van de inhoud van de privacyverklaring van de AP