



AUTORITEIT PERSOONSGEGEVENS

Wanneer heeft u de inbreuk gemeld aan de betrokkene(n)?

9-5-2023

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?

De betrokkenen zijn zelf geïnformeerd, omdat zij tevens melder zijn van het lek.

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

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

Ja, namelijk:

Toelichting:

Volgens de functioneel beheerder van ons portaal "mijn dossier" is het risico minimaal voor betrokkenen. De initiële schademelding wordt volgens hem altijd voorafgaand ingevuld. Het is dus niet gebonden aan het dossier. Tevens is de initiële PDF ook in te zien. De nieuwe eigenaar van een object kent daarnaast de vorige eigenaar (in de meeste gevallen) ook al en daarom is volgens de functioneel beheerder een aanpassing van het systeem niet nodig.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

Ja, namelijk:

Toelichting:

Er wordt gekeken of aanpassing mogelijk zijn.

11 Verzenden

Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

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



AUTORITEIT PERSOONSGEGEVENS

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

5.1.2.e

Van: IMG Helpdesk
Verzonden: vrijdag 16 juni 2023 12:56
Aan: IMG Privacy
Onderwerp: RE: PRIVACY!! RE: mail oud bewoner 5.1.2.e maatwerk

Ha 5.1.2.e,

Buiten reikwijdte

Wat ik uit de voorgaande mailtjes haal is dat E-loket ging informeren of het anders kan en daarna stilte. Daarnaast haal ik ook uit de mailwisseling dat het niet wenselijk is maar dat het inzage in de gegevens bestaat uit inzage in persoonsgegevens die al bij beide partijen bekend zijn. Het oordeel of dit wel of niet valt onder datalek laat ik bij jou liggen.

Hopelijk heb je hier iets aan

Met vriendelijke groet,

5.1.2.e

Cascadeplein 10, 9726AD Groningen
Bezoekruimte: Cascadeplein 6, derde verdieping rechts

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: donderdag 15 juni 2023 15:14

Aan: IMG Helpdesk ^{5.1.2.i (contactgegevens)}@schadedoormijnbouw.nl>; 5.1.2.e @schadedoormijnbouw.nl>;

5.1.2.i (contactgegevens)

cc: 5.1.2.e

Onderwerp: RE: PRIVACY!! RE: mail oud bewoner 5.1.2.e maatwerk

Dag collega's

Zijn er al maatregelen getroffen om dit soort gevallen in de toekomst te voorkomen? Ik moet uiterlijk morgen namelijk verantwoording afleggen aan de AP hierover (d.m.v. een melding).

Er is een voorlopige melding gedaan.

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnschade Groningen

Cascadeplein 10 – 9726 AD Groningen

www.schadedoormijnbouw.nl

Van: IMG Helpdesk [5.1.2.i\(contactgegevens\)@schadedoormijnbouw.nl](mailto:5.1.2.i(contactgegevens)@schadedoormijnbouw.nl)>
Verzonden: donderdag 25 mei 2023 13:33
Aan: 5.1.2.e 5.1.2.e@schadedoormijnbouw.nl; IMG Privacy <Privacy@schadedoormijnbouw.nl>; RVO 5.1.2.i (contactgegevens)
Onderwerp: PRIVACY!! RE: mail oud bewoner 5.1.2.e maatwerk
Urgentie: Hoog

Hallo allen,

Bijgevoegd de laatste reactie en uitleg van 5.1.2.e
Samengevat: works-as-designed en hij gaat kijken of er nog iets aan te doen is.
Het versturen van de CC naar de vorige eigenaar kan 5.1.2.e zelf aanpassen.

Ik heb deze zaak ook met 5.1.2.e besproken. 5.2.1

Met vriendelijke groet,

5.1.2.e

Cascadeplein 10, 9726AD Groningen
Bezoekruimte: Cascadeplein 6, derde verdieping rechts

Van: 5.1.2.e@schadedoormijnbouw.nl>
Verzonden: donderdag 25 mei 2023 12:28
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.e 5.1.2.e@schadedoormijnbouw.nl>
Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Dag 5.1.2.e

Ik heb nog geen terugkoppeling ontvangen, 5.1.2.e heb jij een update?

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Antwoordnummer 3061, 8000 WB Zwolle

Werkdagen: dinsdag t/m vrijdag

T 5.1.2.e

www.schadedoormijnbouw.nl



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: donderdag 25 mei 2023 12:05

Aan: ^{5.1.2.e} <5.1.2.e@schadedoormijnbouw.nl>; IMG SL Vraagbaak

5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>

cc: 5.1.2.e

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Dag 5.1.2.e,

Is het probleem inmiddels al opgelost?

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
Verzonden: dinsdag 16 mei 2023 16:37
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; IMG SL Vraagbaak ^{5.1.2.1 (contactgegevens)} <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
cc: 5.1.2.e [redacted]
Onderwerp: RE: mail oud bewoner 5.1.2.e [redacted] maatwerk

Dag 5.1.2.e

Helaas is het nog niet opgelost, ik kreeg zojuist namelijk bijgaande mail van 5.1.2.e [redacted]

Met vriendelijke groet,

5.1.2.e [redacted]

Instituut Mijnbouwschade Groningen

Antwoordnummer 3061, 8000 WB Zwolle

Werkdagen: dinsdag t/m vrijdag

T 5.1.2.e [redacted]

www.schadedoormijnbouw.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd.
Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: dinsdag 16 mei 2023 16:27

Aan: IMG SL Vraagbaak ^{5.1.2.1 (contactgegevens)} <5.1.2.1@schadedoormijnbouw.nl>

cc: 5.1.2.e

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Hee 5.1.2.e,

Zie de e-mail in de bijlage. Het probleem lijkt opgelost te zijn door 5.1.2.e

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: IMG SL Vraagbaak ^{5.1.2.1 (contactgegevens)} <5.1.2.1@schadedoormijnbouw.nl>

Verzonden: maandag 15 mei 2023 11:31

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Hoi 5.1.2.e

Ik laat de desbetreffende collega even bellen met 5.1.2.e. Krijgen wij ook bericht wanneer onderstaande opgelost is?

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

☎ 0800 4444 111

www.schadedoormijnbouw.nl

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: vrijdag 12 mei 2023 16:07

Aan: IMG SL Vraagbaak ^{5.1.2.i (contactgegevens)} [@schadedoormijnbouw.nl](mailto:5.1.2.i@schadedoormijnbouw.nl)>

cc: 5.1.2.e

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Hee 5.1.2.e

Zou je ook aan 5.1.2.e willen verzoeken om de e-mails te verwijderen?

Dank alvast!

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: vrijdag 12 mei 2023 10:41

Aan: IMG Bijkomende Kosten ^{5.1.2.i (contactgegevens)} [@schadedoormijnbouw.nl](mailto:5.1.2.i@schadedoormijnbouw.nl)>; IMG SL Vraagbaak ^{5.1.2.i (contactgegevens)} [@schadedoormijnbouw.nl](mailto:5.1.2.i@schadedoormijnbouw.nl)>; IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.e

5.1.2.i (contactgegevens)

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Dag 5.1.2.e,

Dit vermeende datalek is sinds dinsdag al bij ons onder de aandacht en wordt op dit moment beoordeeld.

Ik verwacht iedereen vanmiddag van een antwoord te kunnen voorzien. 5.1.2.e is op dit moment bezig om het lek te dichten.

Dank voor het doorsturen van onderstaande e-mails 😊

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: IMG Bijkomende Kosten 5.1.2.i (contactgegevens) [@schadedoormijnbouw.nl](mailto:5.1.2.i@schadedoormijnbouw.nl)>

Verzonden: vrijdag 12 mei 2023 10:36

Aan: IMG SL Vraagbaak 5.1.2.i (contactgegevens) [@schadedoormijnbouw.nl](mailto:5.1.2.i@schadedoormijnbouw.nl); IMG Privacy <Privacy@schadedoormijnbouw.nl>

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Hoi 5.1.2.e,

Welke mails door het systeem automatisch worden uitgestuurd is mij niet bekend.

Hebben jullie dit al gemeld bij [@privacy@schadedoormijnbouw.nl](mailto:privacy@schadedoormijnbouw.nl)?

Als dit een datalek is dan is hier een instructie voor:

5.1.2.i

Fijne dag!

Met vriendelijke groeten,

5.1.2.e

Afdeling Bestuurlijke en Juridische Zaken & Schadeafhandeling

T 5.1.2.e

Van: IMG SL Vraagbaak ^{5.1.2.i (contactgegevens)} @schadedoormijnbouw.nl>
Verzonden: donderdag 11 mei 2023 15:09
Aan: IMG Bijkomende Kosten ^{5.1.2.i (contactgegevens)} @schadedoormijnbouw.nl>
Onderwerp: FW: mail oud bewoner 5.1.2.e maatwerk

Beste collega's,

Even jullie aandacht voor onderstaande. 5.1.2.e neemt contact met ons op omdat hij al een tijd e-mails van ons ontvangt waarin hij meegenomen is in de CC. De mails gaan over bijkomende kosten. Wij hebben zowel BAS, MIRA als Topdesk doorgespit maar kunnen niets terugvinden. 5.1.2.e heeft geen lopende of gesloten dossier bij ons. Wij hebben hem gevraagd om die email naar ons door te sturen. De email vind ik nogal merkwaardig:

----- Forwarded message -----

Van: <noreply@schadedoormijnbouw.nl>
Date: di 9 mei 2023 13:29
Subject: Bevestiging Schademeldpunt Groningen Aanvraag vergoeding schade door mijnbouw
5.1.2.e

Geachte 5.1.2.e,

Wij hebben uw aanvraag voor een vergoeding van bijkomende kosten door schade door mijnbouw ontvangen op 09-05-2023 13:29. U ontvangt ook een ontvangstbevestiging per post met meer informatie over de verdere afhandeling van uw aanvraag.

Let op: bonnetjes en rekeningen moet u bewaren tot zes maanden na toekenning.

Meer informatie

Heeft u vragen, kijk dan op www.schadedoormijnbouw.nl. Of neem telefonisch contact met ons op: 0800 4444 111 (gratis).

Met vriendelijke groet,

Voorzitter Instituut Mijnschade Groningen

Dit is een automatisch bericht. Het is niet mogelijk dit bericht te beantwoorden.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen.

De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message.

The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Kan het zijn dat jullie bovenstaande mail hebben uitgestuurd?

Wij horen het graag van jullie

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

☎ 0800 4444 111

www.schadedoormijnbouw.nl

Van: 5.1.2.e <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: donderdag 11 mei 2023 14:24

Aan: IMG SL Vraagbaak <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

5.1.2.e net gesproken en hij is in de cc meegenomen en heeft het van noreply@schadedoormijnbouw.nl. de mail was gericht aan 5.1.2.e

Heeft de mail nu naar ons gestuurd.

Van: IMG SL Vraagbaak <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: donderdag 11 mei 2023 13:54

Aan: 5.1.2.e <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Hoi 5.1.2.e

Samen met 5.1.2.e hebben wij BAS/MIRA doorgespit en wij kunnen niet vinden.

Zou je aan 5.1.2.e willen vragen naar welk email adres wij de mail sturen en zou hij ons ook de email willen doorsturen zodat wij verder kunnen kijken?

Wat mij opvalt is dat je zegt dat hij in de CC wordt meegenomen. Noreply emails die wij uitsturen nemen wij geen CC in mee.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

☎ 0800 4444 111

www.schadedoormijnbouw.nl

Van: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Verzonden: donderdag 11 mei 2023 08:33

Aan: IMG SL Vraagbaak <[redacted]@schadedoormijnbouw.nl>

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Goedemorgen,

Afzender was noreply@schadedoormijnbouw.nl en het ging over BK aanvraag.

5.1.2.e zei dat dit al vaker was gebeurd en er ook eerder contact over heeft gehad, alleen zie ik daar geen notities van en idd. Kan ik ook niks terug vinden.

Met vriendelijke groet,

5.1.2.e

Van: IMG SL Vraagbaak <[redacted]@schadedoormijnbouw.nl>

Verzonden: woensdag 10 mei 2023 13:01

Aan: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Onderwerp: RE: mail oud bewoner 5.1.2.e maatwerk

Hoi 5.1.2.e,

Wat vaag. Ik heb zowel in BAS als in MIRA gezocht om te kijken of ik een e-mail adres van 5.1.2.e tegenkom, maar niet.

Hij zegt de mail is van ons, maar wie was de afzender? (e-mail adres) en wordt er in de mail aangegeven waarom hij meegenomen wordt in de CC?

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

☎ 0800 4444 111

www.schadedoormijnbouw.nl

Van: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
Verzonden: dinsdag 9 mei 2023 14:23
Aan: IMG SL Vraagbaak [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
Onderwerp: mail oud bewoner 5.1.2.e [redacted] maatwerk

Goedendag collega,

Naam: 5.1.2.e [redacted]
BSN: 5.1.1.e [redacted]
Schadeadres: 5.1.2.e [redacted]

Omschrijving van de situatie/vraag:

Oud bewoner 5.1.2.e [redacted] heeft contact opgenomen omdat hij nog steeds mail ontvangt, hij word in de cc meegenomen, heeft vandaag ook weer een mail ontvangen over aanvraag BK kosten, ik zie deze niet terug in BAS.

Met vriendelijke groet,

5.1.2.e [redacted]

Instituut Mijnbouwschade Groninge

Cascadeplein 10, 9726 AD Groningen
Antwoordnummer 3061, 8000 WB Zwolle

T 0800 4444 111

www.schadedoormijnbouw.nl



Met vriendelijke groeten,

5.1.2.e [redacted]



Instituut Mijnbouwschade Groningen

Cascadeplein 10 - Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

T 0800 4444 111

www.schadedoormijnbouw.nl



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages

Datalek 2023.2



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: 5.1.2.e

Melddatum: 15 juni 2023

Meldtijdstip: 11:15

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?

Een nieuwe melding doen van een inbreuk

Wat voor soort datalek melding 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



AUTORITEIT PERSOONSGEGEVENS

Registratienummer van de FG (indien van toepassing)

5.1.2.e

Naam van het bedrijf of de organisatie

Instituut Mijnbouwschade Groningen

Adres

Cascadeplein 10

Postcode

9726 AD

Plaats

Groningen

In welke sector is de organisatie of het bedrijf actief?

Openbaar bestuur

Overig openbaar bestuur

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam

Functie

E-mailadres

Telefoonnummer

Tweede telefoonnummer

Is de melder de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding?

5.1.2.e
Ja

3.3 Andere organisaties

Waren er andere organisaties betrokken bij de inbreuk?

Nee

4 Tijdljn



AUTORITEIT PERSOONSGEGEVENS

4.1 Duurt de inbreuk op dit moment nog voort?

Ja

(Mogelijke) startdatum van de inbreuk

1-6-2023

4.2 Wanneer is het incident ontdekt?

8-6-2023

4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt

De gemachtigde heeft het datalek zelf bij de organisatie gemeld per mail op 8 juni 2023. Op 13 juni is het datalek bij privacy gemeld. Op 15 juni is dit bij de FG gemeld.

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?

13-6-2023

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?

[✓] Persoonsgegevens toegevoegd aan het verkeerde dossier

5.3 Beschrijving van het incident

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

Op 1 juni wordt er een besluit verzonden naar een aanvrager. Aan dit besluit is een machtiging gehecht. Hoewel de juiste gemachtigde op dit document staat, staan er gegevens van een andere aanvrager in de machtiging voor wie het besluit niet is bedoeld. Er staan grotendeels normale persoonsgegevens in de machtiging, er staat echter ook een BSN in van de aanvrager. Het besluit is per post verzonden en staat tevens nog in het online portaal van de aanvrager aan wie het besluit is geadresseerd.



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

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

Naam

Geboortedatum en/of leeftijd

Burgerservicenummer (BSN)

Contactgegevens

Adres en woonplaats

E-mailadres

Telefoonnummer

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 betreft 1 aanvrager wiens gegevens onjuist zijn verstrekt.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

Klanten (huidig en potentieel)

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.

Aanvrager van een schadevergoeding.



AUTORITEIT PERSOONSGEGEVENS

7.3 Is het exacte aantal betrokkenen bekend?

Ja

Het exacte aantal is:

1

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

De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)

Aanzienlijk

Licht uw keuze toe:

BSN in combinatie met NAW-gegevens zijn zeer gevoelig voor misbruik. Derhalve meer dan een beperkt risico, ondanks dat de ontvanger van de persoonsgegevens deze onrechtmatige verstrekking heeft gemeld.



AUTORITEIT PERSOONSGEGEVENS

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?

Nee

Gaat u de inbreuk nog melden aan de betrokkene(n)?

Ja

Aan hoeveel personen wilt u de inbreuk gaan melden?

1

Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?

19-6-2023

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?

Op 1 juni wordt er een besluit verzonden naar een aanvrager. Aan dit besluit is een machtiging gehecht. Hoewel de juiste gemachtigde op dit document staat, staan er gegevens van een andere aanvrager in de machtiging voor wie het besluit niet is bedoeld. Er staan grotendeels normale persoonsgegevens in de machtiging, er staat echter ook een BSN in van de aanvrager. Het besluit is per post verzonden en stond tevens in het online portaal van de aanvrager aan wie het besluit is geadresseerd. Het besluit is uit het portaal van de aanvrager verwijderd.

De ontvanger van de persoonsgegevens heeft het datalek zelf bij ons gemeld. We zijn momenteel aan het onderzoeken wat er mis is gegaan in onze werkwijze. Gezien de mogelijke gevolgen van dit datalek berichten wij u hierover.

+ mogelijke gevolgen, hoe we tot de inschatting van het risico zijn gekomen, contactgegevens FG, klachtmogelijkheid, contactgegevens AP.

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.

Per brief

10.3 Maatregelen om de inbreuk aan te pakken



AUTORITEIT PERSOONSGEGEVENS

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

Nog niet bekend

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

Nog niet bekend

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 informeren.
- 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

1-7-2023

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

5.1.2.e

Van: Bouwes, mr. M.T. (Menno)
Verzonden: donderdag 15 juni 2023 20:03
Aan: 5.1.2.e
CC: IMG Privacy
Onderwerp: Antw: Brief na datalek 5.1.2.e

Beste 5.1.2.e,

Akkoord.

Groeten,
Menno

Van: 5.1.2.e @schadedoormijnbouw.nl>
Datum: 15 juni 2023 om 16:57:57 CEST
Aan: Bouwes, mr. M.T. (Menno) 5.1.2.e <schadedoormijnbouw.nl>
CC: IMG Privacy <Privacy@schadedoormijnbouw.nl>
Onderwerp: Brief na datalek 5.1.2.e

Beste Menno,

Wij hebben per ongeluk de machtiging van 5.1.2.e als bijlage toegevoegd aan een besluit van een andere aanvrager. Met bijgevoegde brief melden wij dit aan de gemachtigde van 5.1.2.e. Gemachtigde is trouwens al op de hoogte omdat hij door beide aanvragers is gemachtigd.

Graag hoor ik of de brief akkoord is.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

5.1.2.e
www.schadedoormijnbouw.nl



> Retouradres Postbus 40009, 8004 DA Zwolle

5.1.2.e

[Redacted]

**Instituut Mijnbouwschade
Groningen**

Cascadeplein 10
9726 AD Groningen

Postbus 40009
8004 DA Zwolle
088 – 042 7220

www.schadedoormijnbouw.nl
fg@schadedoormijnbouw.nl
privacy@schadedoormijnbouw.nl

Datum: 19 juni 2023

Betreft: Melding Autoriteit Persoonsgegevens

Geachte 5.1.2.e

Met deze brief stel ik u als gemachtigde van 5.1.2.e namens het Instituut Mijnbouwschade Groningen (hierna: het Instituut) op de hoogte van een (mogelijk) datalek. Als gevolg daarvan zijn mogelijk persoonsgegevens in handen gekomen van een derde.

Datalek

Het spijt mij u te moeten melden dat per ongeluk de machtiging van 5.1.2.e van 11 mei 2023 als bijlage door het Instituut is toegevoegd aan een besluit van een andere aanvrager. Dat had niet mogen gebeuren. Ik betreur dit ten zeerste en bied 5.1.2.e hierbij mijn oprechte excuses aan. Het Instituut gaat er alles aan doen om dit soort fouten in de toekomst te voorkomen.

Wat is er gebeurd?

De machtiging van 5.1.2.e van 11 mei 2023 is per ongeluk als bijlage door het Instituut toegevoegd aan een besluit van een andere aanvrager. Als gevolg van deze fout zijn de gegevens mogelijk terecht gekomen bij een ontvanger die hier geen inzage in had mogen hebben. Het Instituut heeft na de verzending op 1 juni 2023 de ontvanger verzocht om de machtiging te verwijderen.

Melden bij Autoriteit Persoonsgegevens

Het Burgerservicenummer, naam, geslacht, (e-mail)adres, telefoonnummer en de handtekening van 5.1.2.e staan in de machtiging. Ook vermeldt de machtiging het KVK-nummer, naam, e-mailadres en telefoonnummer van het bedrijf van 5.1.2.e. Daarnaast is het schadeadres en het zaaknummer in de machtiging opgenomen. Daarom heeft het Instituut een melding gedaan bij de Autoriteit Persoonsgegevens. Verder is ook de interne toezichthouder van het Instituut, de Functionaris Gegevensbescherming, op de hoogte gesteld. Het Instituut heeft geen aanwijzingen dat de toezending van de brief een hoog risico oplevert voor de rechten en vrijheden van betrokkenen.

Meer informatie

Ik begrijp goed dat deze brief vragen kan oproepen. Vanzelfsprekend kunt u contact opnemen met het Instituut. Dat kan met 5.1.2.e [redacted], per e-mail (ook voor een telefonische afspraak): 5.1.2.i (contactgegevens) [redacted].

Hoogachtend,

Mr. H.C.D. (Henk) Korvinus
Voorzitter Bestuur IMG

Deze brief is digitaal tot stand gekomen en daarom niet voorzien van een handtekening.

5.1.2.e

Van: IMG Privacy
Verzonden: maandag 26 juni 2023 09:00
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hee 5.1.2.e,

Super opgelost zo! Dank!

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e @schadedoormijnbouw.nl>
Verzonden: maandag 26 juni 2023 08:15
Aan: 5.1.2.i (contactgegevens) IMG Privacy <Privacy@schadedoormijnbouw.nl>
Onderwerp: FW: Terugkoppeling datalek 5.1.2.e (spoed)

Hoi 5.1.2.e,

Vriendelijk bedankt voor de update. @IMG Privacy, ter info!

Met vriendelijke groet,

5.1.2.e

Van: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>
Verzonden: vrijdag 23 juni 2023 16:25
Aan: 5.1.2.e @schadedoormijnbouw.nl>
Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hoi 5.1.2.e,

Het besluit met de machtiging is verwijderd en het besluit zonder machtiging is toegevoegd 😊.
Met dank aan FB.

Met vriendelijke groet,

5.1.2.e

Afdeling Bestuurlijke en Juridische Zaken & Schadeafhandeling

T 5.1.2.e | Donderdag niet aanwezig

Van: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Verzonden: dinsdag 20 juni 2023 08:10

Aan: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>

CC: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Onderwerp: FW: Terugkoppeling datalek 5.1.2.e (spoed)

Hoi 5.1.2.e,

Vriendelijk bedankt voor jouw hulp.

<IMG@schadedoormijnbouw.nl>, ter info. De brief om 5.1.2.e op te hoogte te stellen van het datalek wordt vandaag verstuurd.

Met vriendelijke groet,

5.1.2.e

Van: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>

Verzonden: maandag 19 juni 2023 16:41

Aan: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: FW: Terugkoppeling datalek 5.1.2.e (spoed)

Hoi 5.1.2.e,

De brief staat in de printmap en wordt morgen verstuurd.

Met vriendelijke groet,

5.1.2.e

Afdeling Bestuurlijke en Juridische Zaken & Schadeafhandeling

T 5.1.2.e | Donderdag niet aanwezig

Van: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>

Verzonden: maandag 19 juni 2023 13:30

Aan: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hallo 5.1.2.e

Je verzoek om de brief vandaag te versturen is gemeld onder 5.1.2.e. Wordt vervolgd.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Afdeling Bestuurlijke en Juridische Zaken & Schadeafhandeling

5.1.2.e | Donderdag niet aanwezig

Van: 5.1.2.e <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: maandag 19 juni 2023 08:59

Aan: 5.1.2.i (contactgegevens) <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Urgentie: Hoog

Hoi 5.1.2.e,

Ik heb een brief opgesteld om 5.1.2.e op te hoogte te stellen van het datalek. De brief dient volgens 5.1.2.e uiterlijk op **maandag 19 juni 2023** te zijn verzonden. Zou jij bijgevoegde brief vandaag nog kunnen (laten) versturen vanuit 5.1.2.e Of kan ik beter iemand anders vragen?

Met vriendelijke groet,

5.1.2.e

Van: 5.1.2.i (contactgegevens) <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: vrijdag 16 juni 2023 16:43

Aan: 5.1.2.e <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hallo 5.1.2.e

Je verzoek is gemeld onder 5.1.2.e . Je hoort van ons wanneer er ontwikkelingen zijn.

Met vriendelijke groet,

5.1.2.e

Afdeling Bestuurlijke en Juridische Zaken & Schadeafhandeling

T 5.1.2.e | Donderdag niet aanwezig

Van: 5.1.2.e <[redacted]> <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: donderdag 15 juni 2023 16:52

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.e <[redacted]>
5.1.2.i (contactgegevens) <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

cc: 5.1.2.e <[redacted]>

Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hoi allen,

@5.1.2.i (contactgegevens) is het misschien een mogelijkheid dat er een kopie van het originele besluit in Mira wordt gezet zonder de bijlage? Anders lijkt het mij ontoegankelijk maken van document of de gegevens blurren mij de meest geschikte oplossing. Graag zo spoedig mogelijk, want dit lek blijft nu voortduren.

@IMG Privacy, ik heb het template ingevuld. Ik zal Menno per e-mail vragen akkoord te geven. De ondertekening in de brief heb ik aangepast naar de huidige voorzitter. Na accordering zal ik vragen om het dossier te laten versturen vanuit 5.1.2.e .

@5.1.2.e), zou jij kunnen laten weten wanneer je aan de verkeerd geadresseerde hebt verzocht om de papieren versie en alle kopieën van de machtiging te verwijderen? In de brief staat namelijk dat wij de ontvanger hebben verzocht om de machtiging te verwijderen.

Met vriendelijke groet,

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: donderdag 15 juni 2023 15:35

Aan: 5.1.2.e <@schadedoormijnbouw.nl>

cc: 5.1.2.e <@schadedoormijnbouw.nl>; 5.1.2.i (contactgegevens)

<@schadedoormijnbouw.nl>; 5.1.2.e

Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hee 5.1.2.e,

Om antwoord op jouw eerste vraag te geven: Is het misschien een mogelijkheid dat er een kopie van het besluit in Mira wordt gezet zonder de bijlage? Anders lijkt het mij ontoegankelijk maken van document of de gegevens blurren mij de meest geschikte oplossing. Graag zo spoedig mogelijk, want dit lek blijft nu voortduren.

Daarnaast hebben wij een template voor jullie opgesteld. Graag zelf invullen en versturen en indien er dingen onduidelijk kun je ons altijd even of bellen of mailen. Daarnaast dient Menno Bouwes deze brief even te ondertekenen.

Verder zie ik dat jij het datalek z.s.m. heb gemeld. Dank daarvoor. Het lek is echter wel sinds 8 juni bij ons al bekend (zie de mail van 5.1.2.e en de vervolgmil van 5.1.2.e). Daarom zijn wij helaas veel te laat met het melden van dit lek. Verzoek aan allen is om dit in de toekomst **z.s.m. te melden**. Wij zullen ook nog een bericht op Plek plaatsen n.a.v. dit incident.

Wij horen graag van jullie wanneer de brief verzonden is. Deze informatie hebben wij nodig voor de verantwoording aan de AP.

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>
Verzonden: donderdag 15 juni 2023 13:05
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.e <[redacted]@schadedoormijnbouw.nl>
Onderwerp: RE: Terugkoppeling datalek 5.1.2.e (spoed)

Hoi allen,

@5.1.2.e <[redacted]>), zou jij aan de verkeerd geadresseerde willen verzoeken om de papieren versie en alle kopieën van de machtiging te verwijderen?

@5.1.2.e <[redacted]@IMG Privacy>, ik vraag me af of we het besluit mogen verwijderen op grond van de AVG en Awb. Is het voldoende om het besluit dat in Mira staat met de verkeerde machtiging onzichtbaar te maken voor de aanvrager/gemachtigde?

@IMG Privacy, de betrokkene van dit datalek dient per brief te worden geïnformeerd over het lek. Hebben jullie daar een template voor? Ik stel voor om deze brief vanuit het dossier van de betrokkene (5.1.2.e) te verzenden. Wie moet dit oppakken?

Het datalek is op dinsdag 13 juni 2023 om 13:10 uur bij mij gemeld. Ik heb het op dinsdag 13 juni 2023 om 13:28 uur bij @IMG Privacy gemeld. Ik vermoed dat het datalek niet eerder is herkend. Misschien is het goed om het herkennen en melden van een datalek nogmaals onder de aandacht te brengen van de eerste lijn (Serviceloket, zaakbegeleiders e.d.)?

Met vriendelijke groet,

5.1.2.e <[redacted]>

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>
Verzonden: donderdag 15 juni 2023 11:58
Aan: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>
cc: 5.1.2.e <[redacted]>

Onderwerp: Terugkoppeling datalek 5.1.2.e (spoed)
Urgentie: Hoog

Hee 5.1.2.e <[redacted]>,

Bedankt voor het melden van het datalek. Hierbij kom ik terug op onderstaande mailwisseling. Het privacyteam heeft onderstaand datalek geregistreerd. Hierbij krijg je een terugkoppeling.

Advies beveiligingsincident (omschrijving van het incident)

Reg.nr. in datalekregister: 5.1.2.e <[redacted]>
Reg.nr. in zaaksysteem: 5.1.2.e <[redacted]>
Datum melding: 13-06-2023

Feiten

Op 1 juni wordt er een besluit verzonden naar een aanvrager. Aan dit besluit is een machtiging gehecht. Hoewel de juiste gemachtigde op dit document staat, staan er gegevens van een andere aanvrager in de machtiging voor wie het besluit niet is bedoeld. Er staan grotendeels normale persoonsgegevens in de machtiging, er staat echter ook een BSN in van de aanvrager. Het besluit is per post verzonden en staat tevens nog in het online portaal van de aanvrager aan wie het besluit is geadresseerd. Op 8 juni 2023 is het lek bekend geworden bij het Instituut. Op 15 juni 2023 is dit lek gemeld bij de Autoriteit Persoonsgegevens (hierna: AP) De 72 uur meldingstermijn is daarom al verstreken en daarom zijn wij te laat met het melden van het datalek bij de AP.

Datalek?

Van een datalek is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de **ongeoorloofde verstrekking** van of de **ongeoorloofde toegang tot** doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).

Er is sprake van een datalek. Er heeft namelijk een ongeoorloofde verstrekking van persoonsgegevens plaatsgevonden, want er is een document met persoonsgegevens naar een onjuist persoon verzonden (digitaal en per post).

Melding aan de Autoriteit Persoonsgegevens en/of betrokkenen?

Een datalek moet door de verwerkingsverantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 lid 1 AVG). Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor betrokkenen.

Het betreft hier een datalek met grotendeels gewone persoonsgegevens en een gevoelig persoonsgegeven, namelijk het BSN. Nu het lek nog niet is gedicht en een BSN in combinatie met andere gegevens kan worden misbruikt voor verschillende doeleinden, wordt het risico van dit lek als aanzienlijk ingeschat. Daarom is een melding gedaan bij de Autoriteit Persoonsgegevens. Tevens dient betrokkene van dit datalek te worden geïnformeerd over het lek. Dit zal middels een brief ondertekend door Henk Korvinus of Hans Houdijk te worden gedaan. De brief dient uiterlijk op **maandag 19 juni 2023** aanstaande te zijn verzonden. Daarnaast dienen de maatregelen (voorgesteld in de bijlage) z.s.m. te worden opgevolgd.

Tot slot het verzoek dit soort meldingen direct bij het privacyteam te melden. Ten eerste omdat dit een serieus risico betreft voor de betrokkene. Daarnaast is de meldingstermijn verstreken en nu het een aanzienlijk lek betreft, staan wij open voor boetes en andere sancties van de AP.

Advies

Kortom, het privacyteam adviseert om:

1. dit incident wel te kwalificeren als datalek;
2. dit datalek **wel** te melden aan de Autoriteit Persoonsgegevens;
3. dit datalek **wel** te melden aan betrokkene.

Met vriendelijke groet,

5.1.2.e

zig. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Verzonden: dinsdag 13 juni 2023 13:28

Aan: IMG herzieningen <[redacted]@schadedoormijnbouw.nl>; 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

>; IMG

Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e besluit VES van 5.1.2.e <[redacted]> bevat op pagina 2 machtiging van 5.1.2.e <[redacted]>

Hoi allen,

@IMG herzieningen, zou jij een herzien besluit kunnen opstellen met daarin de VSO in plaats van de machtiging? De pauzeknop is geweigerd. Het herziene besluit mag daarom verstuurd worden. Ik kijk het graag eerst nog wel even na.

@5.1.2.e ter info. Is volgens mij al eens eerder gebeurd.

@IMG Privacy, er is sprake van een datalek. Aan het besluit is een machtiging van een andere aanvrager gehecht.

Met vriendelijke groet,

5.1.2.e

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte



Datalek 2023.3

5.1.2.e

Van: Beheer MIRA | Rijkszaak
Verzonden: maandag 10 juli 2023 08:51
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: 5.1.2.e

Categorieën: 5.1.2.e

Dag 5.1.2.e,

Bedoel je het gele bestand?

5.1.2.e

Van: 5.1.2.e @schadedoormijnbouw.nl>
Verzonden: maandag 10 juli 2023 08:47
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.i (contactgegevens)
@schadedoormijnbouw.nl>
cc: 5.1.2.e @schadedoormijnbouw.nl>
Onderwerp: 5.1.2.e

Goedemorgen collega's ,

In bovenstaand dossier staat een foutief gekoppelde document met gevoelige gegevens.

5.1.2.e " het is een samenvatting van de aanvraag met NAW gegevens, gekoppeld op 16-6 en inzichtelijk voor de dossiereigenaar.

@5.1.2.e Kunnen jullie dit document asap verwijderen?
Dank!

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 | 9726 AD Groningen

Antwoordnummer 3061 | 8000 WB Zwolle

T 0800 – 4444 111

M 5.1.2.e

www.schadedoormijnbouw.nl

5.1.2.e

Van: Beheer MIRA | Rijkszaak
Verzonden: maandag 10 juli 2023 11:22
Aan: IMG Privacy
Onderwerp: RE: 5.1.2.e

Categorieën: 5.1.2.e

Dag 5.1.2.e,

Als 5.1.2.e op de 16e in Mijn Dossier had gekeken zou het kunnen zijn dat het gezien is maar zeker weten doe ik niet. We kunnen dat helaas niet achterhalen.

Groet,
5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>
Verzonden: maandag 10 juli 2023 10:23
Aan: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>
Onderwerp: RE: 5.1.2.e

Dag 5.1.2.e,

Nog een kleine vraag hierover. Kan je zien of dit document is gedownload door 5.1.2.e? En is er achter te komen of 5.1.2.e dit document in heeft kunnen zien?

Met vriendelijke groeten,

5.1.2.e

Van: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>
Verzonden: maandag 10 juli 2023 09:38
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.e @schadedoormijnbouw.nl>
cc: 5.1.2.e @schadedoormijnbouw.nl>
Onderwerp: RE: 5.1.2.e

Dag 5.1.2.e

Even ter controle: Kunnen jullie aangeven of dit goedstaat en indien nodig geel arceren wat weg moet. Groet
5.1.2.e

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 09:12

Aan: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>; 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

cc: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Goedemorgen 5.1.2.e,

Bedankt voor het direct oppakken van het verzoek. Klopt het dat er eerder twee aanvraag-documenten in het dossier stonden? Ik zie er namelijk nog steeds een document met de naam "5.1.2.e Aanvraag" in het dossier staan.

Met vriendelijke groeten,

5.1.2.e

[Redacted]

Van: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 08:55

Aan: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>; IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Dag allen,

Het verzoek is uitgevoerd! Kunnen jullie duiden hoe dit issue is ontstaan?

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 08:47

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.i(contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>

cc: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: 5.1.2.e

Goedemorgen collega's ,

In bovenstaand dossier staat een foutief gekoppelde document met gevoelige gegevens.

5.1.2.e " het is een samenvatting van de aanvraag met NAW gegevens, gekoppeld op 16-6 en inzichtelijk voor de dossiereigenaar.

@5.1.2.e Kunnen jullie dit document asap verwijderen?
Dank!

Met vriendelijke groet,

5.1.2.e

[Redacted]

Instituut Mijnbouwschade Groningen

Cascadeplein 10 | 9726 AD Groningen
Antwoordnummer 3061 | 8000 WB Zwolle

T 0800 – 4444 111

5.1.2.e

www.schadedoormijnbouw.nl

Instituut
Mijnbouwschade
Groningen



5.1.2.e

Van: IMG Privacy
Verzonden: maandag 10 juli 2023 13:06
Aan: 5.1.2.e
Onderwerp: RE: 5.1.2.e

Urgentie: Hoog

Goedemiddag 5.1.2.e,

Zou je vandaag nog contact op willen nemen met 5.1.2.e en willen vragen of hij dit document heeft ingezien, dan wel gedownload? Dit is namelijk relevant voor het registreren van dit datalek.

Alvast bedankt!

Met vriendelijke groeten,
5.1.2.e

Van: 5.1.2.e @schadedoormijnbouw.nl>
Verzonden: maandag 10 juli 2023 12:01
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>
Onderwerp: RE: 5.1.2.e

Dag 5.1.2.e,

Zoals 5.1.2.e heeft aangegeven. Issue is ontstaan door de verwarring met de naamaanduiding en opvolgend nummering wat veel op elkaar leek.

Dankjewel voor de snelle aanpak en het verwijderen van het foutieve document.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 | 9726 AD Groningen

Antwoordnummer 3061 | 8000 WB Zwolle

M 5.1.2.e

T 5.1.2.1 (contactgegevens)

www.schadedoormijnbouw.nl



Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 10:14

Aan: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

cc: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>; 5.1.2.e

<5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Dag 5.1.2.e,

Dank voor de verduidelijking! Wij gaan dit datalek registreren.

Met vriendelijke groeten,

5.1.2.e

Van: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 09:20

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>; 5.1.2.e

<5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Inderdaad 5.1.2.e

Je zit er weer lekker op!

[@IMG Privacy](mailto:5.1.2.e@img-privacy.nl)

Het foute document is verwijderd.

Het goede document lijkt er heel erg op, "5.1.2.e", die staat er nog in.

Wat ons meteen richting de oorzaak brengt.

Met vriendelijke groet,

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 09:12

Aan: 5.1.2.i (contactgegevens) <5.1.2.i@schadedoormijnbouw.nl>; 5.1.2.e

<5.1.2.e@schadedoormijnbouw.nl>

cc: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Goedemorgen 5.1.2.e,

Bedankt voor het direct oppakken van het verzoek. Klopt het dat er eerder twee aanvraag-documenten in het dossier stonden? Ik zie er namelijk nog steeds een document met de naam 5.1.2.e in het dossier staan.

Met vriendelijke groeten,

5.1.2.e

5.1.2.e

Van: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>
Verzonden: maandag 10 juli 2023 08:55
Aan: 5.1.2.e @schadedoormijnbouw.nl>; IMG Privacy
<Privacy@schadedoormijnbouw.nl>
cc: 5.1.2.e @schadedoormijnbouw.nl>
Onderwerp: RE: 5.1.2.e

Dag allen,
Het verzoek is uitgevoerd! Kunnen jullie duiden hoe dit issue is ontstaan?

Groet,
5.1.2.e

Van: 5.1.2.e @schadedoormijnbouw.nl>
Verzonden: maandag 10 juli 2023 08:47
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.i (contactgegevens)
@schadedoormijnbouw.nl>
cc: 5.1.2.e @schadedoormijnbouw.nl>
Onderwerp: 5.1.2.e

Goedemorgen collega's ,

In bovenstaand dossier staat een foutief gekoppelde document met gevoelige gegevens.
5.1.2.e " het is een samenvatting van de aanvraag met NAW gegevens, gekoppeld op 16-6 en
inzichtelijk voor de dossiereigenaar.

5.1.2.e Kunnen jullie dit document asap verwijderen?
Dank!

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 | 9726 AD Groningen
Antwoordnummer 3061 | 8000 WB Zwolle

T 0800 - 4444 111

5.1.2.e
www.schadedoormijnbouw.nl

Instituut
Mijnbouwschade
Groningen





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: 5.1.2.e

Melddatum: 10 juli 2023

Meldtijdstip: 15:35

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?

Een nieuwe melding doen van een inbreuk

Wat voor soort datalek melding 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



AUTORITEIT PERSOONSGEGEVENS

Registratienummer van de FG (indien van toepassing)

5.1.2.e

Naam van het bedrijf of de organisatie

Instituut Mijnbouwschade Groningen

Adres

Cascadeplein 10

Postcode

9726 AD

Plaats

Groningen

In welke sector is de organisatie of het bedrijf actief?

Mijnbouw

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam

Functie

E-mailadres

Telefoonnummer

5.1.2.e

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?

Nee

4 Tijdljn

4.1 Duurt de inbreuk op dit moment nog voort?

Nee

(Mogelijke) startdatum van de inbreuk

16-6-2023



AUTORITEIT PERSOONSGEGEVENS

(Mogelijke) einddatum van de inbreuk

10-7-2023

4.2 Wanneer is het incident ontdekt?

10-7-2023

4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt

Bij verwerken van het dossier bleek dat de adresgegevens in het document niet overeenkwamen met de informatie in de interne applicatie (Mira). Daarna is de melding gemaakt bij de PO's en daarna plaatsvervangend FG (vanwege vakantie van huidig FG)

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?

Ja

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?

Persoonsgegevens toegevoegd aan het verkeerde dossier

5.3 Beschrijving van het incident

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

Een samenvatting van een aanvraag is op 16 juni 2023 toegevoegd aan een verkeerd dossier, waarna dit inzichtelijk is geweest in MijnDossier. Dit document is, na ontdekking, verwijderd van de desbetreffende locatie. Er is contact opgenomen met de persoon waarvoor het document beschikbaar was gesteld; Deze gaf aan het document niet te hebben gezien.

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



6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

Naam

Geslacht

Geboortedatum en/of leeftijd

Burgerservicenummer (BSN)

Contactgegevens

Adres en woonplaats

E-mailadres

Telefoonnummer

Financiële gegevens

Bankrekeningnummer / IBAN

Andere financiële gegevens

Namelijk:

Compensatie/vergoeding

Anders

Namelijk:

Dossiernummer en kadastrale gegevens

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



AUTORITEIT PERSOONSGEGEVENS

1

Geef een toelichting op bovengenoemd aantal:

Het gaat om een aanvraag van 1 persoon.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

Anders

Namelijk:

Aanvrager

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.

Persoon die een aanvraag heeft ingediend bij het IMG

7.3 Is het exacte aantal betrokkenen bekend?

Nee

Het minimum aantal betrokkenen is:

1

Het maximum aantal betrokkenen is:

1

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.



[✓] Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)

Beperkt

Licht uw keuze toe:

Persoon aan wie de gegevens beschikbaar heeft gesteld heeft deze gegevens niet daadwerkelijk ingezien. Wel gaat het om een combinatie van BSN + naam en adres, dus vandaar een beperkt risico

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?

Nee

Gaat u de inbreuk nog melden aan de betrokkene(n)?

Ja

Aan hoeveel personen wilt u de inbreuk gaan melden?

1

Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?

12-7-2023

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?

Op 16 juni heeft u een aanvraag gedaan bij het IMG. Van deze aanvraag wordt automatisch een samenvatting gemaakt, welke wordt geüpload in MijnDossier. Deze samenvatting is in het MijnDossier geplaatst van een andere persoon, waar deze tot 10 juli beschikbaar is geweest. Bij het verwerken van de aanvragen werd opgemerkt dat de adresgegevens niet overeenkwamen, waarna dit document is verwijderd.

We zijn momenteel aan het onderzoeken wat er mis is gegaan in onze werkwijze. Gezien de mogelijke gevolgen van dit datalek berichten wij u hierover.

+ mogelijke gevolgen, hoe we tot de inschatting



AUTORITEIT PERSOONSGEGEVENS

van het risico zijn gekomen, contactgegevens FG, klachtmogelijkheid, contactgegevens AP.

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.

Per e-mail

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

Ja, namelijk:

Toelichting:

Verwijderen van het verkeerde document.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

Nee, want:

Toelichting:

Menselijk fout bij koppeling samenvatting aan MijnDossier.

11 Verzenden

Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

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

5.1.2.e

Van: IMG Privacy
Verzonden: dinsdag 11 juli 2023 09:55
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Terugkoppeling 5.1.2.e
Bijlagen: Template melden datalek aan betrokkene (1).DOCX
Urgentie: Hoog

Beste 5.1.2.e,

Bedankt voor het melden van het datalek. Hierbij kom ik terug op onderstaande mailwisseling. Het privacyteam heeft onderstaand datalek geregistreerd. Hierbij krijg je een terugkoppeling.

Advies beveiligingsincident (omschrijving van het incident)

Reg.nr. in datalekregister: 5.1.2.e

Reg.nr. in zaaksysteem: 5.1.2.e

Datum melding: 10-07-2023

Feiten

Op 16 juni 2023 is een document met gevoelige gegevens gekoppeld aan een verkeerd dossier. Het betreft een samenvatting van de aanvraag. Dit document is zichtbaar geweest in MijnDossier. In het document staan onder andere: BSN, NAW-gegevens, dossiernummers en financiële gegevens. Dit datalek is op 10 juli 2023 intern gemeld. Het is niet te achterhalen of derde dit document heeft ingezien. De zaakbegeleider heeft contact opgenomen met derde en die heeft aangegeven het document niet ingezien te hebben.

Datalek?

*Van een datalek is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de **ongeoorloofde verstrekking** van of de **ongeoorloofde toegang** tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).*

Er is sprake van een datalek in de hierboven genoemde zaak. Er heeft namelijk een ongeoorloofde verstrekking van persoonsgegevens plaatsgevonden, want er is een document met persoonsgegevens aan het verkeerde dossier gekoppeld. Het document is zichtbaar geweest voor derde in MijnDossier en het is niet te achterhalen of derde dit document ook daadwerkelijk heeft ingezien.

Melding aan de Autoriteit Persoonsgegevens en/of betrokkenen?

Een datalek moet door de verwerkingsverantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 lid 1 AVG). Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor betrokkenen.

Het betreft onder andere gevoelige persoonsgegevens. Het gaat om de volgende persoonsgegevens: NAW-gegevens, BSN, geboortedatum, geslacht, e-mailadres, telefoonnummer, rekeningnummer, dossiernummers, kadastrale gegevens en gegevens over compensatie/vergoeding. Omdat het gevoelige persoonsgegevens betreft en het onduidelijk is of derde toegang heeft gehad tot deze gegevens, levert dit datalek een risico op voor de rechten en vrijheden van betrokkene. Het datalek zal daarom gemeld worden aan de Autoriteit Persoonsgegevens. Ook zal het datalek aan betrokkene worden gemeld. De Autoriteit Persoonsgegevens geeft namelijk aan dat het bij BSN in combinatie met naam en geboortedatum altijd aan betrokkene moet worden gemeld.

Advies

Kortom, het privacyteam adviseert om:

1. Deze incidenten wel te kwalificeren als datalek;
2. deze datalekken **wel** te melden aan de Autoriteit Persoonsgegevens;
3. deze datalekken **wel** te melden aan betrokkene.

Het datalek dient aan betrokkene gemeld te worden aan de hand van de brief die als bijlage is toegevoegd. @5.1.2.e) zou je dit template willen invullen en z.s.m. versturen naar betrokkene? Menno Bouwes dient deze brief te ondertekenen voordat het verstuurd wordt.

Graag horen wij wanneer de brief is verzonden. Deze informatie hebben wij nodig voor de verantwoording aan de Autoriteit Persoonsgegevens.

Met vriendelijke groeten,

5.1.2.e

5.1.2.e

Van: 5.1.2.e @schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 09:20

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>; 5.1.2.e @schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Inderdaad 5.1.2.e,

Je zit er weer lekker op!

@IMG Privacy

Het foute document is verwijderd.

Het goede document lijkt er heel erg op, 5.1.2.e, die staat er nog in.

Wat ons meteen richting de oorzaak brengt.

Met vriendelijke groet,

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 09:12

Aan: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>; 5.1.2.e @schadedoormijnbouw.nl>

cc: 5.1.2.e @schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Goedemorgen 5.1.2.e,

Bedankt voor het direct oppakken van het verzoek. Klopt het dat er eerder twee aanvraag-documenten in het dossier stonden? Ik zie er namelijk nog steeds een document met de naam 5.1.2.e " in het dossier staan.

Met vriendelijke groeten,

5.1.2.e

5.1.2.e

Van: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>

Verzonden: maandag 10 juli 2023 08:55

Aan: 5.1.2.e @schadedoormijnbouw.nl>; IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.e @schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e

Dag allen,

Het verzoek is uitgevoerd! Kunnen jullie duiden hoe dit issue is ontstaan?

Groet,

5.1.2.e

Van: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
Verzonden: maandag 10 juli 2023 08:47
Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>; 5.1.2.i (contactgegevens)
[redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
cc: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>
Onderwerp: 5.1.2.e [redacted]

Goedemorgen collega's ,

In bovenstaand dossier staat een foutief gekoppelde document met gevoelige gegevens.
"5.1.2.e [redacted]" het is een samenvatting van de aanvraag met NAW gegevens, gekoppeld op 16-6 en inzichtelijk voor de dossiereigenaar.

5.1.2.e [redacted] Kunnen jullie dit document asap verwijderen?
Dank!

Met vriendelijke groet,

5.1.2.e [redacted]
[redacted]

Instituut Mijnbouwschade Groningen
Cascadeplein 10 | 9726 AD Groningen
Antwoordnummer 3061 | 8000 WB Zwolle

T 0800 – 4444 111

M 5.1.2.e [redacted]

www.schadedoormijnbouw.nl





> Retouradres Postbus 40009, 8004 DA Zwolle

**Instituut Mijnbouwschade
Groningen**

Cascadeplein 10
9726 AD Groningen

Postbus 40009
8004 DA Zwolle
088 – 042 7220
www.schadedoormijnbouw.nl
fg@schadedoormijnbouw.nl
privacy@schadedoormijnbouw.nl

5.1.2.e

Datum: 13 juli 2023

Betreft: informatie met betrekking tot een datalek inzake 5.1.2.e

Geachte 5.1.2.e,

Met deze brief stel ik u namens het Instituut Mijnbouwschade Groningen (hierna: het Instituut) op de hoogte van een (mogelijke) datalek. Als gevolg daarvan zijn mogelijk persoonsgegevens in handen gekomen van een derde.

Datalek

Het spijt mij u te moeten melden dat per ongeluk een samenvatting van uw aanvraag door het Instituut is toegevoegd aan de digitale dossieromgeving van een andere aanvrager. Dat had niet mogen gebeuren. Ik betreur dit ten zeerste en bied u hierbij mijn oprechte excuses aan. Het Instituut gaat er alles aan doen om dit soort fouten in de toekomst te voorkomen.

Wat is er gebeurd?

Op 16 juni 2023 is een document met gevoelige gegevens gekoppeld aan een verkeerd dossier. Het betreft een samenvatting van de aanvraag. Dit document is zichtbaar geweest in MijnDossier.

Als gevolg van deze fout zijn de gegevens mogelijk terecht gekomen bij een ontvanger die hier geen inzage in had mogen hebben. De zaakbegeleider heeft contact opgenomen met derde en die heeft aangegeven het document niet ingezien te hebben.

Melden bij Autoriteit Persoonsgegevens

In het document staan onder andere: BSN, NAW-gegevens, dossiernummers en financiële gegevens. Dit datalek is op 10 juli 2023 intern gemeld. Daarom heeft het Instituut een melding gedaan bij de Autoriteit Persoonsgegevens. Verder is ook de interne toezichthouder van het Instituut, de Functionaris Gegevensbescherming, op de hoogte gesteld. Het Instituut heeft geen aanwijzingen dat de toevoeging van uw samenvatting een hoog risico oplevert voor de rechten en vrijheden van u als persoon.

Meer informatie

Ik begrijp goed dat deze brief vragen kan oproepen. Vanzelfsprekend kunt u contact opnemen met het Instituut. Dat kan met 5.1.2.e [redacted], per e-mail (ook voor een telefonische afspraak): 5.1.2.i (contactgegevens)

Met vriendelijke groet,

5.1.2.e

Mr. H.C.D. (Henk) Korvinus Voorzitter Bestuur IMG

Datalek 2023.4

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 17 juli 2023 16:57
Aan: 5.1.2.e
CC: IMG Privacy; 5.1.2.e
Onderwerp: RE: Toegekende BZ en HZ na een afwijzing vanwege BVT

Categorieën: 5.1.2.e

Hi 5.1.2.e,

Ik heb de mail verwijderd, ook uit mijn deleted items folder. Ik had het bestand niet gedownload.

5.1.2.e is tot maandag op vakantie en zal daarvoor om die reden dus waarschijnlijk niet reageren.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

From: 5.1.2.e @schadedoormijnbouw.nl>
Sent: Monday, July 17, 2023 3:33 PM
To: 5.1.2.e
Cc: IMG Privacy <Privacy@schadedoormijnbouw.nl>
Subject: RE: Toegekende BZ en HZ na een afwijzing vanwege BVT
Importance: High

Sommige personen die dit bericht hebben ontvangen, ontvangen niet vaak e-mail van 5.1.2.e @schadedoormijnbouw.nl. [Meer informatie over waarom dit belangrijk is](#)

Hoi 5.1.2.e

Vanochtend heb ik onderstaande e-mail met een bijlage naar o.a. jullie gemaild, maar dit had niet gemogen. Ik heb een melding gemaakt van een datalek en in het kader daarvan wil ik jullie graag verzoeken om het bestand (indien gedownload) te verwijderen uit de downloads + uit de prullenbak. Ook mijn mail graag verwijderen + uit de prullenbak.

Kunnen jullie een reactie geven op deze e-mail als de stappen zijn uitgevoerd?

Alvast bedankt.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726AD Groningen

T 5.1.2.e

www.schadedoormijnbouw.nl

Van: 5.1.2.e)

Verzonden: maandag 17 juli 2023 08:40

Aan: 5.1.2.e

cc: 5.1.2.e

Onderwerp: RE: Toegekende BZ en HZ na een afwijzing vanwege BVT

Goedemorgen allen,

Tot nu toe hebben zich 765 mensen teruggetrokken uit de procedure (zie bijlage). Als ik verder voor iemand nog iets kan betekenen dan hoor ik het wel!

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

T 5.1.2.e

www.schadedoormijnbouw.nl

Buiten reikwijdte

Buiten reikwijdte



Buiten reikwijdte



Buiten reikwijdte



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: **5.1.2.e**

Melddatum: 18 juli 2023

Meldtijdstip: 14:04

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?

Een nieuwe melding doen van een inbreuk

Wat voor soort datalek melding 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



AUTORITEIT PERSOONSGEGEVENS

Registratienummer van de FG (indien van toepassing)

5.1.2.e

Naam van het bedrijf of de organisatie

Instituut Mijnbouwschade Groningen

Adres

Cascadeplein 10

Postcode

9726 AD

Plaats

Groningen

In welke sector is de organisatie of het bedrijf actief?

Mijnbouw

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam

Functie

E-mailadres

Telefoonnummer

5.1.2.e

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?

Nee

4 Tijdljn

4.1 Duurt de inbreuk op dit moment nog voort?

Onbekend

(Mogelijke) startdatum van de inbreuk

17-7-2023



AUTORITEIT PERSOONSGEGEVENS

4.2 Wanneer is het incident ontdekt?

17-7-2023

4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt

De veroorzaker heeft het lek zelf bij de organisatie gemeld per e-mail, nadat deze door een andere medewerker op de hoogte werd gesteld dat er een datalek had plaatsgevonden.

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?

Ja

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?

E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?

Ja

5.3 Beschrijving van het incident

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

Een advocatenkantoor stuurde twee documenten met personen die gestopt waren met een gerechtelijke procedure tegen het NAM in het kader van waardedaling en immateriële schade. Ontvanger werd verzocht een aantal personen door te geven, maar uiteindelijk werden de documenten doorgestuurd. Dit werd ook doorgestuurd naar medewerkers van een extern bureau op het gebied van consultancy, technologie en data.

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



6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

Naam

Contactgegevens

Adres en woonplaats

Anders

Namelijk:

Deelnemersnummers

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

1,342

Geef een toelichting op bovengenoemd aantal:

Het ging in dit geval om twee bestanden waarin de persoonsgegevens stonden: een van 765 personen en een andere met 577 personen. De personen in het bestand met 577 lijken volledig overeen te komen met de personen in het bestand met 765 personen.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

Anders

Namelijk:

Deelnemers die zich teruggetrokken hebben uit een gerechtelijke procedure tegen het NAM

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.



AUTORITEIT PERSOONSGEGEVENS

Het betrof een lijst met personen die zich terug hadden getrokken uit een gerechtelijke procedure

tegen het NAM.

7.3 Is het exacte aantal betrokkenen bekend?

Ja

Het exacte aantal is:

765

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.

Identiteitsdiefstal of -fraude

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)

Beperkt

Licht uw keuze toe:

Het gaat in dit geval om voor- en achternamen, adressen en deelnemernummers van de betrokken personen. Het betreft dus geen gevoelige, bijzondere of strafrechtelijke persoonsgegevens. In deze context gaat het wel om gegevens verbandhoudende met een gerechtelijke procedure en terugtrekking daaruit. Deze gegevens zijn gedeeld met twee vertrouwelijke ontvangers. 1 ontvangers heeft dit al definitief verwijderd, de



AUTORITEIT PERSOONSGEGEVENS

andere ontvanger is op dit moment afwezig en leest daarom zijn e-mail niet.

Doordat het gaat om ongeveer 765 personen

waarvan de gegevens zijn gedeeld gaat het om een groot aantal betrokkenen. In combinatie met het soort gegevens en de vertrouwelijke ontvangers is het risico daarom beperkt.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?

Nee

Gaat u de inbreuk nog melden aan de betrokkene(n)?

Nee

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.

[✓] De maatregelen die ik heb getroffen voordat de inbreuk plaatsvond bieden voldoende bescherming om de melding aan de betrokkene(n) achterwege te kunnen laten

Welke maatregelen heeft u getroffen waardoor het niet nodig is om de betrokkenen te informeren?

De ontvangers gevraagd om de e-mails direct definitief te verwijderen en dit te bevestigen.

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

Ja, namelijk:

Toelichting:

Ontvangers verzocht de e-mails definitief te verwijderen (ook uit de prullenbak) en dit te bevestigen.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

Nee, want:

Toelichting:

Het betreft een menselijke fout. Veroorzaker is zich bewust van de gevolgen van haar handelen en gaat in de toekomst voorzichtiger om met persoonsgegevens.



AUTORITEIT PERSOONSGEGEVENS

11 Verzenden

Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

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

5.1.2.e

Van: 5.1.2.e
Verzonden: woensdag 19 juli 2023 13:50
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Memo 5.1.2.e motivatie melden Datalek

Hierbij de memo van 5.1.2.e

Situatie

In de ochtend van 17 juli is er een Excel bestand gedeeld met twee externen die geen toegang dienden te hebben tot de gegevens. Dit is aan te merken als een datalek, specifiek een inbreuk op vertrouwelijkheid. De bestanden bevatten de voor- en achternamen, adresgegevens en bewoner- en deelnemer nummers van respectievelijk 765 en 577 personen. Het gaat om personen die zich hebben teruggetrokken uit een gerechtelijke procedure m.b.t. waardedaling en immateriële schadevergoeding tegen het NAM. De ontvangers zijn verzocht de bestanden te verwijderen (ook uit de prullenbak) en dit te bevestigen. Eén ontvanger heeft dit tot nu toe gedaan, de andere ontvanger is met vakantie.

Melding aan de Autoriteit Persoonsgegevens

Datalekken, zoals bovenstaande, dienen aan de Autoriteit Persoonsgegevens gemeld te worden voor zover het waarschijnlijk is dat er een risico is voor de rechten en vrijheden van betrokkenen. Een mogelijk risico is in dit geval al voldoende. De beoordeling of er sprake is van een risico heeft in dit geval plaatsgevonden op basis van de volgende factoren.

De eerste factor is het soort gegevens. In de basis gaat om zogenoemde 'normale' persoonsgegevens. Echter, gezien de context waar de gegevens betrekking op hebben, krijgen deze een meer gevoelig karakter. Het gaat immers om persoonsgegevens van personen die zich hebben teruggetrokken uit een gerechtelijke procedure. Dit heeft automatisch tot gevolg dat het risico voor betrokkenen hoger moet worden ingeschat; hoe gevoeliger de gegevens, hoe hoger het risico.

De tweede factor is de identificeerbaarheid van personen. Omdat het om o.a. om namen en adressen gaat, is het voor onbevoegden direct mogelijk om deze personen te identificeren. Hiervoor hoeven geen aanvullende gegevens achterhaald te worden. Hierdoor is er een groter risico voor betrokkenen op misbruik van persoonsgegevens.

De derde factor is de omvang van persoonsgegevens. Ongeacht het daadwerkelijke aantal personen, 765 of 1342 of ergens daartussenin, betreft het een grote groep personen van wie persoonsgegevens zijn gelekt. Vanzelfsprekend is het risico op misbruik door onbevoegden groter wanneer er meer persoonsgegevens zijn gelekt.

Bovenstaande zorgt ervoor dat er altijd enig risico is voor de personen van wie gegevens onbedoeld zijn gedeeld. Dit risico kan bestaan uit het gevoeliger worden voor fraude en het (bijdragen aan) identiteitsfraude. Of dit risico zich daadwerkelijk

verwezenlijkt is niet van belang. Voorgaande is de reden dat het datalek is gemeld bij de Autoriteit Persoonsgegevens.

Melding aan betrokkenen

In sommige gevallen dienen betrokkenen op de hoogte te worden gesteld. Hiervan is sprake wanneer er een waarschijnlijk hoog risico is. In de huidige situatie is daarvan geen sprake. De ontvangers zijn in dit geval verzocht om de gegevens te verwijderen, waarbij één ontvanger dit ook daadwerkelijk al heeft gedaan. Deze ontvangers zijn daarbij ook aan te merken als een vertrouwelijke ontvanger, omdat ze een duurzame relatie hebben met het IMG. Hierdoor mag ervan uit worden gegaan dat ze daadwerkelijk handelen zoals gevraagd.

5.1.2.e

Van: IMG Privacy
Verzonden: woensdag 19 juli 2023 11:31
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Terugkoppeling melding datalek

Goedemorgen 5.1.2.e

Bedankt voor het melden van het datalek. Hierbij kom ik terug op onderstaande mailwisseling. Het privacyteam heeft onderstaand datalek geregistreerd. Hierbij krijg je een terugkoppeling.

Advies beveiligingsincident NAM-procedure lijsten

Reg.nr. in datalekregister: 5.1.2.e

Reg.nr. in zaaksysteem: n.v.t.

Datum melding: 17-07-2023

Feiten

Een advocatenkantoor stuurde een document met personen die gestopt waren met een gerechtelijke procedure tegen het NAM in het kader van waardedaling en immateriële schade periodiek door naar het IMG. Op 17 juli 2023 is deze lijst per ongeluk naar medewerkers van een extern bureau doorgestuurd. De ontvangers is gevraagd het document en de mail (definitief) te verwijderen zodat zij hier geen beschikking meer over hebben.

Datalek?

*Van een datalek is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de **ongeoorloofde verstrekking** van of de **ongeoorloofde toegang** tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).*

Er is sprake van een datalek in de hierboven genoemde zaak. Er heeft namelijk een ongeoorloofde verstrekking van persoonsgegevens plaatsgevonden, want er is een document met gegevens naar personen buiten het IMG gegaan.

Melding aan de Autoriteit Persoonsgegevens en/of betrokkenen?

Een datalek moet door de verwerkingsverantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 lid 1 AVG). Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor betrokkenen.

Het datalek is door ons onderzocht en gezien de hoeveelheid persoonsgegevens en de context van de lijst is dit lek bij de Autoriteit Persoonsgegevens gemeld. Een melding bij betrokkenen kan achterwege blijven nu het lek geen hoog risico meebrengt voor betrokkenen.

Advies

Kortom, het privacyteam adviseert om:

1. Dit incident wel te kwalificeren als datalek;
2. dit datalek **wel** te melden aan de Autoriteit Persoonsgegevens;
3. dit datalek **niet** te melden aan betrokkenen.

Met vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <[redacted]>@schadedoormijnbouw.nl>

Verzonden: maandag 17 juli 2023 13:34

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Onderwerp: Melding datalek

Urgentie: Hoog

Hoi collega's,

Ik wil graag melding doen van een datalek. Ik heb een reply op een e-mail gegeven en daarbij een lijst met namen en adressen gedeeld van mensen die zich hebben teruggetrokken uit een gerechtelijke procedure. Hierbij heb ik over het hoofd gezien dat dit ook naar twee personen is gegaan die niet bij het IMG werken.

Als jullie verder nog informatie nodig hebben, dan hoor ik het graag.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

T 5.1.2.e
www.schadedoormijnbouw.nl

Van: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>

Verzonden: maandag 17 juli 2023 13:23

Aan: 5.1.2.e

Onderwerp: RE: Toegekende BZ en HZ na een afwijzing vanwege BVT

Urgentie: Hoog

Hi allen,

Dank voor de lijst 5.1.2.e

Ik zie wel dat je deze (ik denk per abuis) ook naar de 5.1.2.e e-mailadressen van 5.1.2.e hebt gestuurd. Dat lijkt mij niet de bedoeling. Ik denk goed als jullie daar zelf de juiste acties op ondernemen bij IMG enerzijds en 5.1.2.e anderzijds.

Groet,
5.1.2.e

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726AD Groningen
Antwoordnummer 3016 – 8000 WB Zwolle

T 5.1.2.e
www.schadedoormijnbouw.nl



From: 5.1.2.e <5.1.2.e@schadedoormijnbouw.nl>
Sent: maandag 17 juli 2023 08:40

To: 5.1.2.e

Cc: 5.1.2.e

Subject: RE: Toegekende BZ en HZ na een afwijzing vanwege BVT

Goedemorgen allen,

Tot nu toe hebben zich 765 mensen teruggetrokken uit de procedure (zie bijlage). Als ik verder voor iemand nog iets kan betekenen dan hoor ik het wel!

Met vriendelijke groet,

5.1.2.e

Instituut Mijnschade Groningen
Cascadeplein 10 – 9726AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

T 5.1.2.e

www.schadedoormijnbouw.nl

Buiten reikwijdte

Buiten reikwijdte



Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Buiten reikwijdte

Datalek 2023.5

5.1.2.e

Van: Beheer MIRA | Rijkszaak
Verzonden: dinsdag 12 september 2023 14:12
Aan: IMG Privacy
CC: 5.1.2.e
Onderwerp: RE: datalek, verwijderen verkeerde koppeling. 5.1.2.e

Categorieën: 5.1.2.e

Hoi 5.1.2.e,

Het document heb ik verwijderd!

Zie schermafbeelding hieronder. Het document is voorvertoond en door intermediair gedownload.



5.1.2.e

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10, 9726 AD Groningen

Antwoordnummer 3061, 8000 WB Zwolle

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: dinsdag 12 september 2023 13:59

Aan: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>

Onderwerp: RE: datalek, verwijderen verkeerde koppeling. 5.1.2.e

Goedemiddag collega's,

Zouden jullie onderstaand verzoek met spoed op willen pakken? In het verkeerd gekoppelde FAG staan veel persoonsgegevens, dus het is van belang dat deze zo snel mogelijk uit het verkeerde dossier wordt gehaald.

5.1.2.e

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e @schadedoormijnbouw.nl>

Verzonden: dinsdag 12 september 2023 09:21

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

CC: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>

Onderwerp: datalek, verwijderen verkeerde koppeling. 5.1.2.e

Beste ,

Zie dossiernummer:

Collega heeft verkeerde FAG gekoppeld aan dossier.

Melding gedaan door intermediair met de vraag dit z.s.m. te verwijderen.

Bij deze het verzoek.

Zie voor meer info volgende printscreen:

In de cc 5.1.2.e meegenomen i.v.m. verwerking van het technische verzoek.

5.1.2.e

5.1.2.e

Met vriendelijke groet,

5.1.2.e

[Redacted signature block]

Instituut Mijnbouwschade Groningen

Techniekweg 1 – 9601 MD Hoogezand

Antwoordnummer 3061– 8000 WB Zwolle

T 5.1.2.e

www.schadedoormijnbouw.nl



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages



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: **5.1.2.e**

Melddatum: 13 september 2023

Meldtijdstip: 14:20

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?

Een bestaande melding aanvullen of aanpassen

Beschikt u over het meldingsnummer van de oorspronkelijke melding?

Ja

Dit is het meldingsnummer:

5.1.2.e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam

Functie

E-mailadres

Telefoonnummer

5.1.2.e

2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling

Ja



3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

[✓] Samenvatting van het incident

6. Betrokken persoonsgegevens

[✓] Welke persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

10. Vervolgacties

5.3 Beschrijving van het incident

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

Op 5 september 2023 is door een medewerker het verkeerde formulier aanvullende gegevens (FAG) in een dossier geüpload. In dit FAG stonden NAW, telefoonnummer, e-mailadres, geslacht gegevens van gemachtigde en machtiger en een BSN van de machtiger (aanvrager). In het betreffende dossier treed een intermediair voor de aanvrager op. Deze intermediair heeft het verkeerd gekoppelde document ingezien en heeft



AUTORITEIT PERSOONSGEGEVENS

na ontdekking van het verkeerde document contact opgenomen met het instituut. De intermediair heeft een e-mail gestuurd op vrijdag 8-9-2023. De betreffende medewerker was op vrijdag vrij, waardoor de melding pas op maandag is gezien. Hij heeft de intermediair toen direct

verzocht het document te verwijderen. De melding is op dinsdag doorgezet naar het privacyteam van het IMG, waarnaar functioneer beheer direct is verzocht om het document te verwijderen.

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

6 Betrokken persoonsgegevens

6.1 Persoonsgegevens in het algemeen

Naam

Geslacht

Burgerservicenummer (BSN)

Contactgegevens

Adres en woonplaats

E-mailadres

Telefoonnummer

6.2 Bijzondere categorieën van persoonsgegevens

Meerdere opties zijn mogelijk.

11 Verzenden

Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

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.



AUTORITEIT
PERSOONSGEGEVENS

Privacyverklaring

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

5.1.2.e)

Van: IMG Privacy
Verzonden: donderdag 14 september 2023 10:15
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Memo gemeld datalek aan de AP
Bijlagen: Memo melden datalek 14092023.pdf

Goedemorgen 5.1.2.e,

Gisteren heb je contact gehad met mijn collega 5.1.2.e over een datalek die we hebben gemeld aan de Autoriteit Persoonsgegevens. 5.1.2.e is vandaag niet aan het werk, dus vandaar dat ik de Memo voor management en persvoorlichting naar je stuur. De Memo is geschreven door 5.1.2.e en is toegevoegd als bijlage.

Mocht je nog vragen hebben, dan horen we het graag!

Met vriendelijke groeten,

5.1.2.e

5.1.2.e

5.1.2.e . Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Situatie

Op 12 september 2023 is bij het privacy team via de mail melding gemaakt van een datalek. In de mail werd melding gemaakt van een formulier aanvullende gegevens (FAG) dat op 5 september 2023 in een verkeerd dossier is opgenomen. De intermediair die in dit dossier optreedt heeft dit op 8 september 2023 per mail gemeld. De desbetreffende medewerker was op die dag afwezig, waardoor de mail pas op 11 september 2023 werd opgepakt en op 12 september is verstuurd naar het privacy team.

Na onderzoek blijkt het te gaan om een machtigingsformulier dat niet volledig is ingevuld. Het formulier is in de FAG opgenomen. Op het formulier zijn NAW-gegevens, telefoonnummer en e-mailadres van zowel de machtiger als de gemachtigde ingevuld. Het BSN van de machtiger is ook ingevuld op het FAG. Het formulier is daarnaast ook ondertekent door de machtiger. Het privacy team heeft direct contact opgenomen met het functioneel beheer van Mira die het document uit het dossier hebben gehaald. Daarbij bleek dat het document is ingezien, maar ook gedownload is door de onbevoegde intermediair. De intermediair is verzocht dit document te verwijderen.

Melding aan de Autoriteit Persoonsgegevens

Datalekken, zoals bovenstaande, dienen aan de Autoriteit Persoonsgegevens gemeld te worden voor zover het waarschijnlijk is dat er een risico is voor de rechten en vrijheden van betrokkenen. Een mogelijk risico is in dit geval al voldoende. De beoordeling of er sprake is van een risico heeft in dit geval plaatsgevonden op basis van de volgende factoren.

De eerste factor is het soort gegevens. In deze casus gaat het naast "gewone" persoonsgegevens zoals naam en adres ook om gevoelige persoonsgegevens, namelijk het BSN van de machtiger (aanvrager). Dat er gevoelige persoonsgegevens, in combinatie met verschillende andere persoonsgegevens zijn gelect, levert in dit specifieke geval een mogelijk risico op.

De tweede factor is de identificeerbaarheid van personen. Omdat het om o.a. om namen en adressen gaat, is het voor onbevoegden direct mogelijk om deze personen te identificeren. Hiervoor hoeven geen aanvullende gegevens achterhaald te worden. Hierdoor is risico voor betrokkenen op misbruik van persoonsgegevens vergroot.

De derde factor is de omvang van persoonsgegevens. In dit datalek gaat het om de persoonsgegevens van twee personen. De omvang van de groep betrokkenen van dit datalek valt daarom mee.

Bovenstaande punten zijn meegenomen in de afweging van het risico. In de basis is er een groot risico voor betrokkene, met name de machtiger. Echter, omdat de intermediair het datalek heeft gemeld en is verzocht om het document te verwijderen, resteert een gemiddeld risico voor betrokkenen. Dit omdat het BSN-nummer in combinatie met een grote hoeveelheid andere gegevens over een specifieke persoon zijn gelect en fraude met deze gegevens mogelijk blijft. Of dit risico zich daadwerkelijk verwezenlijkt is niet van belang. Voorgaande is de reden dat het datalek is gemeld bij de Autoriteit Persoonsgegevens.

Melding aan betrokkenen

In sommige gevallen dienen betrokkenen op de hoogte te worden gesteld. Hiervan is sprake wanneer er een waarschijnlijk hoog risico is. In de huidige situatie is daarvan geen sprake. De ontvanger is in dit geval verzocht om de gegevens te verwijderen, waarbij ontvanger heeft aangegeven dit te doen. Omdat het om een intermediair gaat is het risico op misbruik van de gegevens als niet heel groot aan te merken.

5.1.2.e

Van: IMG Privacy
Verzonden: vrijdag 15 september 2023 09:29
Aan: 5.1.2.e)
Onderwerp: Terugkoppeling datalek, verwijderen verkeerde koppeling. 5.1.2.e

Hallo 5.1.2.e

Bedankt voor het melden van het datalek. Hierbij kom ik terug op onderstaande mailwisseling. Het privacyteam heeft onderstaand datalek geregistreerd. Hierbij krijg jij een terugkoppeling.

Advies verkeerde FAG
Reg.nr. in datalekregister: 5.1.2.e
Reg.nr. in zaaksysteem: . 5.1.2.e
Datum melding: 12-09-2023

Feiten

Op 5 september 2023 is er een FAG aan een verkeerd dossier toegevoegd. Intermediair, die inzage heeft in het dossier heeft dit op 8 september aangegeven. Het verkeerde document is op 12 september verwijderd uit het dossier. Het betreft De verkeerde ontvanger heeft dit datalek zelf bij ons gemeld. Er kan daarom aangenomen worden dat de verkeerde ontvanger geen kwade bedoelingen heeft. In het FAG stonden echter naast gewone persoonsgegevens ook een BSN, dit is een gevoelig persoonsgegeven.

Datalek?

Van een datalek is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens (artikel 4, punt 12, AVG).

Er is sprake van een datalek in de hierboven genoemde zaak. Er heeft namelijk een ongeoorloofde verstrekking van persoonsgegevens plaatsgevonden, want de FAG is door een onbevoegde ingezien en gedownload.

Melding aan de Autoriteit Persoonsgegevens en/of betrokkenen?

Een datalek moet door de verwerkingsverantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 lid 1 AVG). Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor betrokkenen.

Wij hebben dit datalek gemeld bij de Autoriteit omdat er naast gewone persoonsgegevens ook een BSN bij de verkeerde ontvanger terecht is gekomen. Een BSN is een gevoelig persoonsgegeven, waardoor dit een hoger risico voor de betrokkene oplevert. We hebben het datalek niet bij de betrokkene gemeld, nu het datalek door de intermediair zelf is gemeld.

Advies

Kortom, het privacyteam adviseert om:

1. Dit incident wel te kwalificeren als datalek;
2. Dit datalek te melden aan de Autoriteit Persoonsgegevens;
3. Dit datalek niet te melden aan betrokkene.

Nogmaals dank voor het op de hoogte stellen over dit datalek, hierdoor hebben we de benodigde acties kunnen nemen: Functioneel Beheer heeft het document uit het dossier gehaald en intermediair is verzocht het document te verwijderen.

Met vriendelijke groet,

5.1.2.e

privacy@schadedoormijnbouw.nl zijn. Bij mijn afwezigheid kunt u bij

Instituut Mijnschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle



Van: 5.1.2.e [redacted]@schadedoormijnbouw.nl>

Verzonden: dinsdag 12 september 2023 09:21

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

CC: 5.1.2.i (contactgegevens) [redacted]@schadedoormijnbouw.nl>

Onderwerp: datalek, verwijderen verkeerde koppeling. 5.1.2.e

Beste ,

Zie dossiernummer:

Collega heeft verkeerde FAG gekoppeld aan dossier.

Melding gedaan door intermediair met de vraag dit z.s.m. te verwijderen.

Bij deze het verzoek.

Zie voor meer info volgende printscreen:

In de cc 5.1.2.e meegenomen i.v.m. verwerking van het technische verzoek.

5.1.2.e

5.1.2.e

Met vriendelijke groet,

5.1.2.e

[Redacted signature block]

Instituut Mijnbouwschade Groningen

Techniekweg 1 – 9601 MD Hoogezand

Antwoordnummer 3061– 8000 WB Zwolle

T 5.1.2.e

www.schadedoormijnbouw.nl

Datalek 2023.6

5.1.2.e

Van: IMG Privacy
Verzonden: donderdag 28 september 2023 16:01
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: terugkoppeling 5.1.2.e mogelijk datalek

Hi 5.1.2.e,

Bedankt voor ons gesprek van zonet. Hierbij kom ik terug op onderstaande mailwisseling. Het privacyteam heeft onderstaand datalek geregistreerd. Hierbij krijg jij een terugkoppeling.

Advies beveiligingsincident (omschrijving van het incident)

Reg.nr. in datalekregister: 5.1.2.e

Reg.nr. in zaaksysteem: 5.1.2.e

Datum melding: 26-09-2023

Feiten

Op 7 maart 2023 zijn de bijgevoegde stukken zijn in tweevoud aan de rechtbank toegezonden (voorblad calculatie, expertiserapport en keuzeformulier). Op deze stukken zijn de volgende gegevens van de vorige bewoner zichtbaar:

- Naam;
- Mobiel nummer;
- E-mailadres;
- IBAN;
- Handtekening.

Deze stukken zijn per abuis niet gelakt en de nieuwe bewoner 5.1.2.e heeft een afschrift van deze stukken ontvangen. De rechtbank is tevens in het bezit van deze stukken. Dit document is verstuurd door beroep en is per koerier afgeleverd op voornoemde datum. De nieuwe bewoner heeft beroep ingesteld en vandaar dat een afschrift van de stukken is toegezonden.

Datalek?

*Van een datalek is sprake bij een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de **ongeoorloofde verstrekking** van of de **ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens** (artikel 4, punt 12, AVG).*

Er is sprake van een datalek in de hierboven genoemde zaak. Er heeft namelijk een ongeoorloofde verstrekking van persoonsgegevens plaatsgevonden, aangezien de gegevens van de vorige bewoner niet zijn gelakt.

Melding aan de Autoriteit Persoonsgegevens en/of betrokkenen?

Een datalek moet door de verwerkingsverantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 lid 1 AVG). Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor betrokkenen.

In deze casus gaat het naast "gewone" persoonsgegevens zoals naam en adres ook om gevoelige persoonsgegevens, namelijk IBAN en handtekening van de vorige bewoner. Dat er gevoelige persoonsgegevens, in combinatie met verschillende andere persoonsgegevens zijn gelekt, levert in dit specifieke geval een mogelijk risico op. Om deze reden wordt het datalek gemeld aan de Autoriteit Persoonsgegevens. Dit datalek hoeft niet gemeld te worden aan betrokkene, aangezien de ontvangers van de stukken in dit geval de rechtbank en de nieuwe bewoner zijn, die naar alle waarschijnlijkheid het document al kent dan wel onder zich heeft.

Advies

Kortom, het privacyteam adviseert om:

1. Deze incidenten wel te kwalificeren als datalek;
2. deze datalekken **wel** te melden aan de Autoriteit Persoonsgegevens;
3. deze datalekken **niet** te melden aan betrokkene.

Zojuist heb ik ook met 5.1.2.e gesproken. Aangezien het in dit geval gaat om de rechtbank, hoeven de gelakte stukken niet opnieuw bij de rechtbank worden ingediend. We kunnen het voor nu dan ook hierbij laten.

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e @schadedoormijnbouw.nl>

Verzonden: donderdag 28 september 2023 13:29

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.e ; 5.1.2.i (contactgegevens)

@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e mogelijk datalek

Beste 5.1.2.e

Ik heb je zojuist gebeld, maar ik kreeg geen gehoor. Zou je mij terug willen bellen zodat we het onderhavige kunnen bespreken?

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

Niet aanwezig op vrijdag

T 5.1.2.e

www.schadedoormijnbouw.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd.

Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's

verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: donderdag 28 september 2023 11:41

Aan: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

cc: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>; 5.1.2.i (contactgegevens)

<[redacted]@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e mogelijk datalek

Hi 5.1.2.e,

Dank voor je reactie. Wij hebben nog twee aanvullende vragen. Is het mogelijk om te achterhalen of 5.1.2.e de stukken heeft verkregen bij de overdracht van zijn huis. Is het daarnaast nog mogelijk om nieuwe gelakte stukken bij de rechtbank in te dienen?

Alvast veel dank!

Met vriendelijke groet,

5.1.2.e

[redacted]. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Verzonden: woensdag 27 september 2023 07:58

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

cc: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>; 5.1.2.i (contactgegevens)

<[redacted]@schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e mogelijk datalek

Beste 5.1.2.e,

In verband met de afwezigheid van 5.1.2.e, reageer ik namens hem. Afgelopen maandag is bekend geworden dat gegevens van de vorige bewoner nog zichtbaar waren. Wellicht wel goed om te weten dat 5.1.2.e vermoedelijk de NAM-stukken al kent dan wel in zijn bezit had. Daarbij van uitgaande dat de stukken ter beschikking zijn gesteld tijdens de overdracht van de woning via de makelaar.

Met vriendelijke groet,

5.1.2.e

Van: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Verzonden: dinsdag 26 september 2023 16:14

Aan: 5.1.2.i (contactgegevens) @schadedoormijnbouw.nl>

Onderwerp: RE: 5.1.2.e mogelijk datalek

Hi 5.1.2.e,

Veel dank voor het melden van dit datalek. Op dit moment zijn we het datalek aan het onderzoeken. Hiervoor hebben we nog wat extra informatie nodig: wanneer is het bekend geworden dat in de stukken de gegevens van de vorige bewoner nog zichtbaar waren?

Alvast bedankt!

Met vriendelijke groet,

5.1.2.e

. Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnschade Groningen

Cascadeplein 10 – 9726 AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

Van: 5.1.2.e @schadedoormijnbouw.nl> Namens IMG beroep schade

Verzonden: dinsdag 26 september 2023 16:06

Aan: IMG Privacy <Privacy@schadedoormijnbouw.nl>

Onderwerp: 5.1.2.e mogelijk datalek

Dag collega's,

Hierbij meld ik een mogelijk datalek inzake dossier 5.1.2.e

De bijgevoegde stukken zijn op 7 maart 2023 in tweevoud aan de rechtbank toegezonden (voorblad calculatie, expertiserapport en keuzeformulier). Op deze stukken zijn de volgende gegevens van de vorige bewoner zichtbaar:

- Naam;
- Mobiel nummer;
- E-mailadres;
- IBAN;
- Handtekening.

Deze stukken zijn per abuis niet gelakt en de nieuwe bewoner 5.1.2.e) heeft een afschrift van deze stukken ontvangen. De rechtbank is tevens in het bezit van deze stukken. Dit document is verstuurd door beroep en is per koerier afgeleverd op voornoemde datum. 5.1.2.e heeft beroep ingesteld en vandaar dat een afschrift van de stukken is toegezonden.

Wij horen graag van jullie.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl



Cascadeplein 10
9726 AD Groningen

Antwoordnummer 3061
8000 WB Zwolle

0800 44 44 111
contact@schadedoormijnbouw.nl

memo

Situatie

Op 26 september 2023 is bij het privacy team via de mail melding gemaakt van een datalek. In de mail werd melding gemaakt van stukken daterend uit 2015 die op 7 maart 2023 in tweevoud naar de rechtbank zijn toegezonden (voorblad calculatie, expertiserapport en keuzeformulier). Op deze stukken zijn de volgende gegevens van de vorige bewoner zichtbaar: naam, adres, mobiel nummer, e-mailadres, IBAN en handtekening. Op 25 september 2023 is bij het Instituut bekend geworden dat de gegevens van de vorige bewoner nog zichtbaar waren.

Deze stukken zijn per abuis niet gelakt en de nieuwe bewoner (eigenaar 5.1.2.e) heeft een afschrift van deze stukken ontvangen. De rechtbank is tevens in het bezit van deze stukken. Dit document is verstuurd door beroep en is per koerier afgeleverd op 7 maart 2023. De nieuwe bewoner heeft beroep ingesteld en vandaar dat een afschrift van de stukken is toegezonden. De betreffende afdeling geeft hierbij aan dat de nieuwe bewoner vermoedelijk deze stukken al kent dan wel in zijn bezit had. Daarbij uitgaande dat de stukken ter beschikking zijn gesteld tijdens de overdracht van de woning via de makelaar.

Melding aan de Autoriteit Persoonsgegevens

Datalekken, zoals bovenstaande, dienen aan de Autoriteit Persoonsgegevens gemeld te worden voor zover het waarschijnlijk is dat er een risico is voor de rechten en vrijheden van betrokkenen. Een mogelijk risico is in dit geval al voldoende. De beoordeling of er sprake is van een risico heeft in dit geval plaatsgevonden op basis van de volgende factoren.

De eerste factor is het soort gegevens. In deze casus gaat het naast "gewone" persoonsgegevens zoals naam en adres ook om gevoelige persoonsgegevens, namelijk IBAN en handtekening van de vorige bewoner. Dat er gevoelige persoonsgegevens, in combinatie met verschillende andere persoonsgegevens zijn gelect, levert in dit specifieke geval een mogelijk risico op.

De tweede factor is de identificeerbaarheid van personen. Omdat het om o.a. om namen en adressen gaat, is het voor onbevoegden direct mogelijk om deze personen te identificeren. Hiervoor hoeven geen aanvullende gegevens achterhaald te worden. Hierdoor is risico voor betrokkenen op misbruik van persoonsgegevens vergroot.

De derde factor is de omvang van persoonsgegevens. In dit datalek gaat het om de persoonsgegevens van één persoon. De omvang van de groep betrokkenen van dit datalek valt daarom mee.

Bovenstaande punten zijn meegenomen in de afweging van het risico. In de basis is er een groot risico voor betrokkene. Echter, omdat de nieuwe bewoner waarschijnlijk de betreffende stukken al kent dan wel in zijn bezit had, resteert een gemiddeld risico voor betrokkenen. Dit omdat het IBAN en handtekening in combinatie met een grote hoeveelheid andere gegevens over een specifieke persoon zijn gelect en fraude met deze gegevens mogelijk blijft. Of dit risico zich daadwerkelijk verwezenlijkt is niet van belang. Voorgaande is de reden dat het datalek is gemeld bij de Autoriteit Persoonsgegevens.

Melding aan betrokkenen

In sommige gevallen dienen betrokkenen op de hoogte te worden gesteld. Hiervan is sprake wanneer er een waarschijnlijk hoog risico is. In de huidige situatie is daarvan geen sprake. De

ontvangers zijn in dit geval de rechtbank en de nieuwe bewoner, die naar alle waarschijnlijkheid het document al kent dan wel onder zich heeft.



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: 5.1.2.e

Melddatum: 28 september 2023

Meldtijdstip: 14:29

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?

Een bestaande melding aanvullen of aanpassen

Beschikt u over het meldingsnummer van de oorspronkelijke melding?

Ja

Dit is het meldingsnummer:

5.1.2.e

2 Aanvulling op eerdere samenvatting

2.1 Wie dient de aanvulling in?

Naam

Functie

E-mailadres

Telefoonnummer

5.1.2.e

2.2 Is de indiener de contactpersoon met wie de Autoriteit Persoonsgegevens contact kan opnemen voor nadere informatie over de melding en aanvulling

Ja



3 Welke vragen

3.1 Welke vragen wilt u wijzigen of aanvullen?

Bij het indienen van een vervolgmelding krijgt u een leegformulier te zien, ook als u een correct meldnummer invult. Om de vertrouwelijkheid van de melding te waarborgen, zijn deze gegevens niet online te bekijken.

Geef daarom per gekozen hoofdstuk en paragraaf de actuele en volledige informatie op over de melding. Selecteer bijvoorbeeld onder Persoonsgegevens alle persoonsgegevens die bij het datalek zijn betrokken.

Wilt u alleen uw melding definitief maken en verandert u niks aan andere onderdelen van de melding? Dan vraagt de AP u een toelichting te geven waarom de melding enkel definitief wordt gemaakt. Deze toelichting kunt u plaatsen onder “Samenvatting van het incident”, onderdeel van Hoofdstuk 5 “Gegevens over de inbreuk”.

1. Introductie

2. Grensoverschrijdende inbreuk

3. De verwerkingsverantwoordelijke

4. Tijdlijn

5. Gegevens over de inbreuk

6. Betrokken persoonsgegevens

7. Getroffen personen

8. Maatregelen vooraf

9. Gevolgen

Gevolgen voor de betrokkene(n) (Persoon of personen van wie gegevens zijn getroffen door de inbreuk)

10. Vervolgacties

Maatregelen om de inbreuk aan te pakken?

9 Gevolgen

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

Identiteitsdiefstal of -fraude

9.3 Inschatting risico



AUTORITEIT PERSOONSGEGEVENS

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)

Beperkt

Licht uw keuze toe:

Het gaat in dit geval om 'normale' persoonsgegevens, maar ook het IBAN en de handtekening van de oude bewoner. Er niet sprake is van een 'betrouwbare' ontvanger. Wel had de bewoner deze stukken al in zijn bezit had, omdat deze verkregen waren bij de overdracht van het huis. Hierdoor is fraude altijd potentieel mogelijk.

10 Vervolgacties naar aanleiding van de inbreuk

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

Nee, want:

Toelichting:

De bewoner heeft de stukken verkregen bij de overdracht van het huis en was dus al in bezit van deze persoonsgegevens. De stukken bij de rechtbank waren niet nieuw.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

Ja, namelijk:

Toelichting:

Er is extra aandacht gevestigd op dit soort gevallen en het lakken van documenten voor verstrekking.

11 Verzenden

Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

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

2023.7

Van: 5.1.2.e
Aan: 5.1.2.e
Cc: 5.1.2.e
Onderwerp: RE: Datalek
Datum: dinsdag 14 maart 2023 10:40:37
Bijlagen: [image001.jpg](#)

Goedemorgen 5.1.2.e

Fijn, bedankt.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels



Van: 5.1.2.e @schadedoormijnbouw.nl>
Verzonden: dinsdag 14 maart 2023 10:38
Aan: 5.1.2.e @schadedoormijnbouw.nl>
cc: 5.1.2.e @schadedoormijnbouw.nl>
Onderwerp: FW: Datalek

Goedemorgen 5.1.2.e,

Bedankt voor het melden van een (mogelijk) datalek.
We gaan het datalek registreren en analyseren.

Fijn dat jij de verkeerde ontvanger hebt verzocht de ontvangen mail te verwijderen.

Mochten er nog verdere acties nodig zijn, dan laten we je dat weten.

Tot slot zou ik je willen verzoeken om datalekken voortaan via privacy@schadedoormijnbouw.nl te melden.

Dank alvast, vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

5.1.2.e

www.schadedoormijnbouw.nl

5.1.2.e

IMG_logo 300 pixels



Van: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Verzonden: maandag 13 maart 2023 17:54

Aan: 5.1.2.e <[redacted]@schadedoormijnbouw.nl>

Onderwerp: Datalek

Goedemiddag,

Ik heb bijgaande mail naar een verkeerd e-mailadres verstuurd. Het juiste e-mailadres is 5.1.2.e

Voor de zekerheid heb ik deze persoon verzocht de mail te verwijderen. De mail is uiteraard ook alsnog naar het juiste e-mailadres verstuurd. Kan ik verder nog iets doen?

De persoonsgegevens die mogelijk bij de verkeerde persoon terecht zijn gekomen, zijn de namen en het adres van eisers.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels



Van: 5.1.2.e
Aan: 5.1.2.e
Cc: 5.1.2.e 5.1.2.e 5.1.2.e
Onderwerp: RE: Datalek
Datum: donderdag 16 maart 2023 11:31:06
Bijlagen: [image001.jpg](#)

Dag 5.1.2.e,

Zoals besproken levert dit datalek geen risico op. Wel is het zo netjes om betrokkene hierover te informeren.

Indien de geadresseerde waaraan de gegevens zijn gelekt een bevestiging van verwijdering van de gegevens aan jou stuurt, ontvangen wij graag deze e-mail van jou.

Met vriendelijke groet,

5.1.2.e

Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels



Van: 5.1.2.e @schadedoormijnbouw.nl>

Verzonden: dinsdag 14 maart 2023 10:41

Aan: 5.1.2.e @schadedoormijnbouw.nl>

cc: 5.1.2.e @schadedoormijnbouw.nl>

Onderwerp: RE: Datalek

Goedemorgen 5.1.2.e,

Fijn, bedankt.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels



Van: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: dinsdag 14 maart 2023 10:38

Aan: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

cc: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Onderwerp: FW: Datalek

Goedemorgen 5.1.2.e,

Bedankt voor het melden van een (mogelijk) datalek.
We gaan het datalek registreren en analyseren.

Fijn dat jij de verkeerde ontvanger hebt verzocht de ontvangen mail te verwijderen.

Mochten er nog verdere acties nodig zijn, dan laten we je dat weten.

Tot slot zou ik je willen verzoeken om datalekken voortaan via privacy@schadedoormijnbouw.nl te melden.

Dank alvast, vriendelijke groet,

5.1.2.e [redacted]

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

5.1.2.e [redacted]

www.schadedoormijnbouw.nl

5.1.2.e [redacted]

IMG_logo 300 pixels



Van: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Verzonden: maandag 13 maart 2023 17:54

Aan: 5.1.2.e [redacted] <[\[redacted\]@schadedoormijnbouw.nl](mailto:[redacted]@schadedoormijnbouw.nl)>

Onderwerp: Datalek

Goedemiddag,

Ik heb bijgaande mail naar een verkeerd e-mailadres verstuurd. Het juiste e-mailadres is **5.1.2.e**

Voor de zekerheid heb ik deze persoon verzocht de mail te verwijderen. De mail is uiteraard ook alsnog naar het juiste e-mailadres verstuurd. Kan ik verder nog iets doen?

De persoonsgegevens die mogelijk bij de verkeerde persoon terecht zijn gekomen, zijn de namen en het adres van eisers.

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen

Cascadeplein 10 – 9726AD Groningen

Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels





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: **5.1.2.e**

Melddatum: 17 maart 2023

Meldtijdstip: 16:57

1 Introductie

1.1 De melding van een inbreuk

Wat wilt u doen?

Een nieuwe melding doen van een inbreuk

Wat voor soort datalek melding 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



AUTORITEIT PERSOONSGEGEVENS

Naam van het bedrijf of de organisatie

Instituut Mijnbouwschade Groningen

Adres

Cascadeplein 10

Postcode

9726 AD

Plaats

Groningen

In welke sector is de organisatie of het bedrijf actief?

Openbaar bestuur

Overig openbaar bestuur

3.2 Gegevens melder en contactpersoon

Wie meldt de inbreuk?

Naam

Functie

E-mailadres

Telefoonnummer

5.1.2.e

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?

Nee

4 Tijdslijn

4.1 Duurt de inbreuk op dit moment nog voort?

Ja

(Mogelijke) startdatum van de inbreuk

13-3-2023



AUTORITEIT PERSOONSGEGEVENS

4.2 Wanneer is het incident ontdekt?

14-3-2023

4.3 Geef (kort) aan hoe u de inbreuk heeft ontdekt

Een medewerker van het Instituut Mijnbouwschade Groningen (hierna: het Instituut) heeft op maandag 13/3/ 2023 om 17:54 uur een mail gestuurd naar de afdeling Informatiebeveiliging en Privacy met de mededeling dat zij per abuis een mail heeft verzonden naar een onjuist geadresseerde met een inhoudelijk verweerschrift en een ontvangstbevestigingsbrief. Op dinsdag 14 maart 2023 heeft de Afdeling Informatiebeveiliging en Privacy onderzoek ingesteld naar het datalek om 10:38 uur.

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?

Ja

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?

E-mail met persoonsgegevens verstuurd aan verkeerde ontvanger(s)

Heeft de verkeerde ontvanger bevestigd de e-mail te hebben verwijderd?

De verkeerde ontvanger heeft niet gereageerd

5.3 Beschrijving van het incident

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

Op maandag 13/3/2023 om 17:54 meldt een medewerker van het Instituut dat zij per abuis een e-mail met als bijlagen een inhoudelijk verweerschrift en een ontvangstbevestigingsbrief van de Rechtbank heeft verzonden. In het verweerschrift (zie bijlage) staan de volgende persoonsgegevens: namen en adres burgers,



AUTORITEIT PERSOONSGEGEVENS

namen juristen, namen deskundigen, handtekening advocaat, schadebedrag beslissing op aanvraag schadebedrag beslissing op bezwaar en dossiernummers. Op dinsdag 14/3/2023 om 10.38 uur is er onderzoek ingesteld door het Instituut. Er is gecontroleerd of de gegevens daadwerkelijk zijn verzonden naar een verkeerd e-mailadres. Er is tevens gepoogd om te onderzoeken of het e-mailadres waartoe de gegevens zijn verzonden daadwerkelijk bestond. Na de vaststelling dat het e-mailadres daadwerkelijk bestond, heeft het Instituut getracht om in contact te komen met de geadresseerde. Er is een e-mail verzonden met het verzoek om de vorige e-mail te verwijderen.

Vervolgens zijn de risico's van het lek

geanalyseerd. Er staan grotendeels alleen gewone persoonsgegevens in het verweerschrift. Daarnaast staan er enkele gevoelige persoonsgegevens (schadebedragen en informatie over rechtspositie) in het verweerschrift. Om die reden is na intern overleg toch besloten om dit datalek aan bij de Autoriteit Persoonsgegevens te melden. Gelet op de enkele gevoelige persoonsgegevens die zijn gelekt en het niet reageren van de geadresseerde waaraan de gegevens zijn gelekt, is er sprake van een risico voor betrokkene. Een rechtspositie van een betrokkene dient alleen kenbaar te worden gemaakt aan de procespartijen en de rechtbank. Gelet op de stilte aan de kant van de geadresseerde is ook niet vast te stellen of geadresseerde als betrouwbaar is aan te merken.

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

6 Welke persoonsgegevens

6.1 Persoonsgegevens in het algemeen

Naam

Geslacht

Contactgegevens

Adres en woonplaats

Financiële gegevens

Andere financiële gegevens

Namelijk:

toegekende schadevergoeding beslissing op aanvraag en beslissing op bezwaar

Anders

Namelijk:

informatie over rechtspositie, schade gerelateerde kenmerken



AUTORITEIT PERSOONSGEGEVENS

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

8

Geef een toelichting op bovengenoemd aantal:

Per categorie persoonsgegevens (zie ook vorige toelichtingen) heb ik het aantal persoonsgegevens opgesomd. Indien dit uitgebreider moet, doen wij dat graag.

7 Getroffen personen

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

Meerdere opties zijn mogelijk.

Werknemers

Anders

Namelijk:

burgers

7.2 Geef een nadere omschrijving van de groep(en) betrokkenen.

Het betreft persoonsgegevens van de burger die in beroep zijn gegaan tegen een beslissing op bezwaar van het Instituut, medewerkers van het Instituut (juristen, bestuursvoorzitter), een advocaat van Pels Rijcken en andere medewerkers van het Instituut (deskundigen die schadeopnames doen).

7.3 Is het exacte aantal betrokkenen bekend?

Ja

Het exacte aantal is:

11

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

[✓] De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt

9.2 (Mogelijke) gevolgen voor de betrokkene(n)

Meerdere opties zijn mogelijk.

[✓] Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens

9.3 Inschatting risico

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkene(n)

Aanzienlijk

Licht uw keuze toe:

Er bestaat naar mening van het Instituut een hoog risico voor betrokkenen. Er zijn namelijk gegevens gelect die worden beschermd door het beroepsgeheim. De meeste gegevens die gelect zijn bestaan echter wel uit gewone persoonsgegevens. De meeste betrokkenen waarvan de gegevens zijn gelect die zijn in het kader van de uitvoering van hun werk betrokken bij dit lek.

De gevoelige financiële gegevens die zijn gelect betreffen alleen uitgekeerde vergoedingen, die niet kunnen leiden tot enig frauduleus handelen dan wel financiële verliezen. Hoewel het niet fraai is dat een rechtspositie van een burger is gelect, is dit risico enigszins beperkt nu het alleen gelect is aan één persoon. Ook meent het Instituut dat dit lek verder geen nadelige invloed zal hebben op de rechtspositie van de burger in zijn zaak tegen het Instituut. Het Instituut zal verder trachten om contact te blijven zoeken met de geadresseerde



AUTORITEIT PERSOONSGEGEVENS

van dit e-mailadres en blijven verzoeken om het e-mailbericht met bijlagen te verwijderen.

10 Vervolgacties naar aanleiding van de inbreuk

10.1 Informeren van de betrokkene(n)

Heeft u de inbreuk reeds gemeld aan de betrokkene(n)?

Nee

Gaat u de inbreuk nog melden aan de betrokkene(n)?

Ja

Aan hoeveel personen wilt u de inbreuk gaan melden?

3

Wanneer gaat u (naar verwachting) de inbreuk melden aan de betrokkene(n)?

20-3-2023

Licht toe aan welke (groep) betrokkenen u de inbreuk heeft gemeld:

De betrokken burgers zullen worden ingelicht over het datalek

Wat is de inhoud van de melding aan degene van wie gegevens zijn gelekt?

Zie vorige pagina's.

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

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:

Het betreffen gewone persoonsgegevens van de overige betrokkenen die in het kader van hun werk betrokken zijn bij dit lek.



AUTORITEIT PERSOONSgegevens

10.3 Maatregelen om de inbreuk aan te pakken

Heeft uw organisatie maatregelen getroffen om de inbreuk aan te pakken?

Ja, namelijk:

Toelichting:

Verzocht om de e-mail te verwijderen.

Heeft uw organisatie maatregelen getroffen om nieuwe soortgelijke inbreuken te voorkomen?

Ja, namelijk:

Toelichting:

Het beroepenteam is op de hoogte van het lek en neemt maatregelen om dit te voorkomen. Het is besproken in een teamoverleg en de medewerkers zullen hier extra scherp op zijn.

11 Verzenden

Is dit een voorlopige of een definitieve melding?

Ja, de melding is definitief. Ik heb de vereiste informatie verstrekt en er is geen vervolgmelding nodig

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

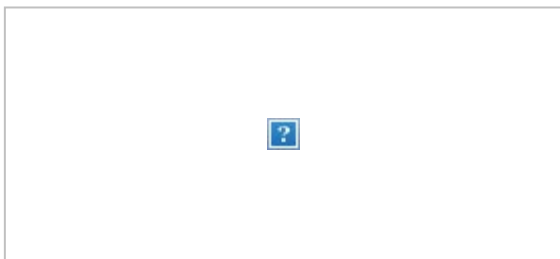
Ik ben op de hoogte van de inhoud van de [Privacyverklaring](#) van de AP

Van: 5.1.2.e
Aan: [IMG Privacy](#)
Cc: 5.1.2.i (contactgegevens)
Onderwerp: Brief
Datum: donderdag 23 maart 2023 16:56:56
Bijlagen: [image001.jpg](#)
[Brief aan 5.1.2.e](#) [_23-03-2023.pdf](#)
[image003.jpg](#)
[image007.jpg](#)

Beste 5.1.2.e,

Deze brief heb ik zojuist van het secretariaat van de heer Kortmann ontvangen. Zorg jij voor de verzending van de brief per e-mail aan de gemachtigde, 5.1.2.e. Privacyvragen van betrokkenen kunnen worden doorgeleid aan 5.1.2.e, heb ik begrepen.

De gegevens van de gemachtigde (kopie uit opgave in dossier) heb ik hieronder opgenomen:



5.1.2.e



Kan jij separaat een afschrift van de brief, na de verzending aan betrokkenen, ter informatie toezenden aan de zaakbegeleider, 5.1.2.e

Met vriendelijke groet,

5.1.2.e

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels



Dit bericht kan informatie bevatten die niet voor u is bestemd.
Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het

bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages

Van: [IMG Privacy](#)
Aan: 5.1.2.e
Cc: 5.1.2.i (contactgegevens)
Bcc: 5.1.2.e 5.1.2.e
Onderwerp: Brief inzake een (mogelijk) datalek
Datum: donderdag 23 maart 2023 17:21:14
Bijlagen: [image001.jpg](#)
[Brief aan 5.1.2.e](#) [23-03-2023.pdf](#)

Geachte 5.1.2.e ,

Namens de voorzitter van het Instituut Mijnbouwschade Groningen, de heer B. Kortmann, stuur ik u bijgaand een brief. Voor de verdere inhoud van het bericht verwijs ik u naar deze brief.

Ik kan het mij voorstellen dat u nadere vragen heeft naar het lezen van deze brief. Voor vragen kunt u mailen naar het e-mailadres: privacy@schadedoormijnbouw.nl.

Tevens kunt u voor vragen ook terecht bij fg@schadedoormijnbouw.nl (meegenomen in de CC).

Met vriendelijke groet,

5.1.2.e

Bij mijn afwezigheid kunt u bij privacy@schadedoormijnbouw.nl zijn.

Instituut Mijnbouwschade Groningen
Cascadeplein 10 – 9726 AD Groningen
Antwoordnummer 3061 – 8000 WB Zwolle

www.schadedoormijnbouw.nl

IMG_logo 300 pixels



> Retouradres Postbus 40009, 8004 DA Zwolle

5.1.2.e

**Instituut Mijnbouwschade
Groningen**

Cascadeplein 10
9726 AD Groningen

Postbus 40009
8004 DA Zwolle
088 - 042 7220
www.schadedoormijnbouw.nl
fg@schadedoormijnbouw.nl
privacy@schadedoormijnbouw.nl

Datum 23 maart 2023
Betreft Melding Autoriteit Persoonsgegevens

Geachte 5.1.2.e

Met deze brief stel ik u, als gemachtigde van 5.1.2.e, namens het Instituut Mijnbouwschade Groningen (hierna: het Instituut) op de hoogte van een (mogelijke) datalek. Als gevolg daarvan zijn mogelijk persoonsgegevens in handen gekomen van een derde.

Datalek

Het spijt mij u te moeten melden dat per ongeluk een e-mail met als bijlage een brief aan de rechtbank en het verweerschrift (met daarin persoonsgegevens) door het Instituut is verzonden naar een onjuist e-mailadres. Dat had niet mogen gebeuren. Ik betreur dit ten zeerste en bied u hierbij mijn oprechte excuses aan. Het Instituut gaat er alles aan doen om dit soort fouten in de toekomst te voorkomen.

Wat is er gebeurd?

Bij het verzenden van de e-mail is iets niet goed gegaan. Het gaat om een e-mail die aan de rechtbank Noord-Nederland is verstuurd vanaf het account 'IMG beroep schade'

5.1.2.i (contactgegevens)@schadedoormijnbouw.nl) op maandag 13 maart 2023 om 15:17 uur.

Als gevolg van een fout door een medewerker van het Instituut is bij de verzending van de e-mail naar de rechtbank een onjuist e-mailadres in het cc-veld ingevoerd. Het Instituut gebruikt het cc-veld zodat alle procespartijen de correspondentie van het Instituut met de rechtbank op hetzelfde moment ontvangen. Er hoeft dan niet te worden gewacht tot de rechtbank deze correspondentie doorstuurt.

In plaats van de e-mailadressen die u bij de correspondentie over uw dossier heeft gebruikt (te weten: 5.1.2.e en 5.1.2.e) is de e-mail verzonden naar een

onjuist e-mailadres. Dat onjuiste e-mailadres was een samenvoeging van de twee bij het Instituut bekende e-mailadressen. Tijdens het invoeren van het e-mailadres in het cc-veld is deze fout gemaakt.

Als gevolg van deze fout zijn de gegevens mogelijk terecht gekomen bij een ontvanger die hier geen inzage in had mogen hebben. Niet bekend is of deze persoon de e-mail ook daadwerkelijk heeft ontvangen, geopend of gelezen. Het Instituut heeft na de verzending op 13 maart 2023 de ontvanger diezelfde dag per e-mail verzocht om de e-mail ongelezen te verwijderen, maar heeft hierop (nog) geen reactie ontvangen. Mocht het Instituut op een later moment alsnog een reactie ontvangen, dan ontvangt u daarover uiteraard ook bericht.

Melding bij Autoriteit Persoonsgegevens

De e-mail aan de rechtbank, de brief en het verweerschrift bevatten persoonsgegevens. Het gaat onder andere om de NAW-gegevens van 5.1.2.e . Daarom heeft het Instituut een melding gedaan bij de Autoriteit Persoonsgegevens. Verder is ook de interne toezichthouder van het Instituut, de Functionaris Gegevensbescherming, op de hoogte gesteld. Het Instituut heeft geen aanwijzingen dat de toezending van de brief een hoog risico oplevert voor rechten en vrijheden van de betrokkenen. De persoonsgegevens die zijn opgenomen in de e-mail, brief en het onderliggende verweerschrift lenen zich namelijk niet voor misbruik.

Meer informatie

Ik begrijp goed dat deze brief vragen kan oproepen. Vanzelfsprekend kunt u contact opnemen met het Instituut. Dat kan met 5.1.2.e , per e-mail (ook voor een telefonische afspraak): fg@schadedoormijnbouw.nl.

Hoogachtend,

5.1.2.e

S.C.J.J. (Bas) Kortmann
Voorzitter Bestuur Instituut Mijnbouwschade Groningen

Overige documenten



Melden datalekken

Datum	Maandag 28 februari 2022
Versie	D1.0

Colofon

Projectnaam	IMG
Projectnummer	N.v.t.
Versiestatus	Voorlopig Definitief
Versienummer	1.0
Versiedatum	28-02-2022
Locatie	5.1.2.h
Projectleiders	
Contactpersoon	5.1.2e
Bijlage(n)	geen
Auteurs	5.1.2e
Proceseigenaar	5.1.2e
Afdeling	Regiebureau
Vastgesteld op	21-04-2022

Versiebeheer en Vaststelling

Proceseigenaar	5.1.2e		
Procesmanager	5.1.2e		
Status/Versie	Datum	Auteur	Opmerking
Definitief / 1.0	21-4-2022	5.1.2e	Definitieve publicatie
Voorlopig Definitief/ 1.0	8-3-2022	5.1.2e	Ter goedkeuring naar 5.1.2e
Concept/ 0.4	09-02-2022	5.1.2e	Opmerkingen/aanvullingen 5.1.2e verwerkt. <ul style="list-style-type: none"> • Functie 5.1.2.e • Proceseigenaar en Procesmanager omgezet naar het Regiebureau; uitvoerende afdeling van Bedrijfsvoering naar Ontwikkeling & Beheer
Concept / 0.3	9-9-2021	5.1.2e	Procesplaat als voorlopig definitief doorgevoerd
Concept / 0.2	22-06-2021	5.1.2e	Aanvullingen
Concept / 0.1	01-06-2021	5.1.2e	Aanvullingen gemaakt.

Colofon

Proceseigenaar	5.1.2e
Inhoudelijk beheer	5.1.2e

Validatieoverzicht

Status/Versie	Datum	Wie
D 1.0	21-4-2022	5.1.2e
C 0.4	23-02-2022	5.1.2e
C 0.3	27-01-2022	5.1.2e
C 0.2	22-06-2021	5.1.2e
C 0.1	01-06-2021	5.1.2e

Geldigheid

Geldigheidsduur	1 jaar
Evaluatiemoment	Om de 3 maanden of na wijzigingen in het proces

Accordering

Procesmanager	5.1.2e
Datum	08-03-2022

Vaststelling

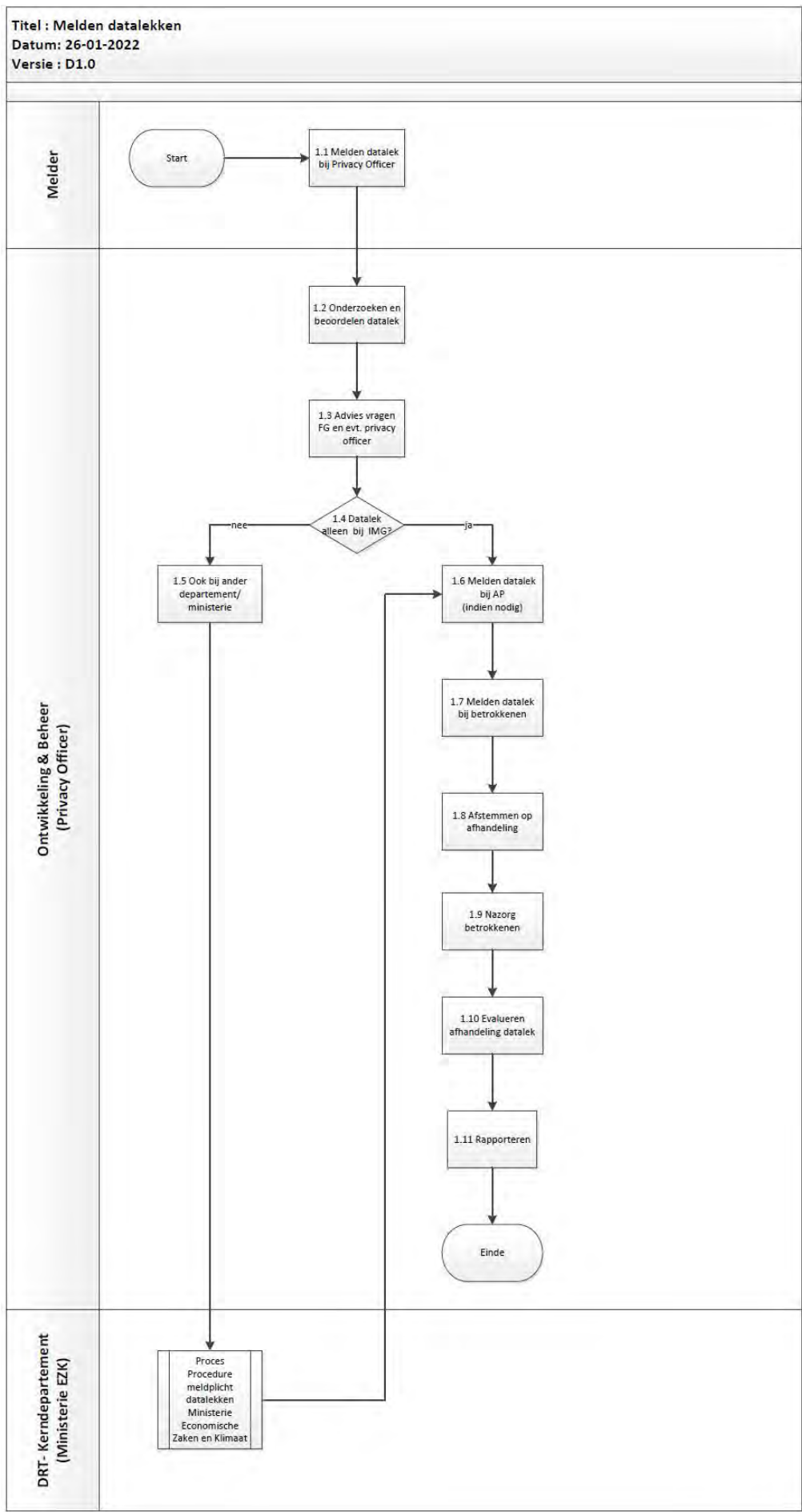
Proceseigenaar	5.1.2e
Datum	21-4-2022

Inhoudsopgave

Colofon.....	2
Inhoudsopgave.....	4
1. Melden datalek	5
1.1. Melden datalek bij Privacy Officer.....	7
1.2. Onderzoeken en beoordelen datalek	7
1.3. Advies vragen FG en evt. privacy jurist.....	8
1.4. Datalek alleen bij IMG?	8
1.5. Ook bij ander departement/ministerie.....	8
1.6. Melden datalek bij AP (indien nodig).....	9
1.7. Melden datalek bij betrokkenen.....	9
1.8. Afstemmen op afhandeling	9
1.9 Nazorg betrokkenen.....	10
1.10 Evalueren afhandeling datalek	10
1.11 Rapporteren	10

1. Melden datalekken

Doel:	Het melden en afhandelen van een datalek	
Omschrijving:	<p>Een datalek is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte (persoons)gegevens (AVG art. 4, lid 12).</p> <p>Hierbij wordt met de vernietiging van persoonsgegevens bedoeld dat de gegevens niet langer bestaan en de beschadiging van gegevens houdt in dat de persoonsgegevens gewijzigd of niet langer volledig zijn. Bij het verlies van persoonsgegevens heeft de Verwerkingsverantwoordelijke niet langer controle over of toegang tot de gegevens. Tenslotte heeft de ongeoorloofde of onrechtmatige verwerking van persoonsgegevens betrekking op het verstrekken van persoonsgegevens aan onbevoegden.</p> <p>Persoonsgegevens; alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon 'de betrokkene' (AVG art. 4 lid 1).</p> <p>Zo'n inbreuk kan vervelende gevolgen hebben voor de personen waarvan gegevens worden verwerkt.</p> <ul style="list-style-type: none"> Voor voorbeelden van een datalek: Zie Procedure Datalekken bladzijde 5 <p>In deze procesbeschrijving is beschreven wie een datalek kan ontdekken en melden, bij wie deze gemeld moet worden en hoe de verdere beoordeling en afhandeling verloopt.</p>	
Trigger:	Het ontvangen van een melding datalek	
Waarmee:	Procedure Datalekken IMG Formulier Datalekken en Incidenten	
Wanneer:	<<Geef aan wanneer dit deelproces uitgevoerd wordt>>	
Wie:	Responsible	Ontwikkeling & Beheer (Privacy Officer), evt. DRT-Kerndepartement (Ministerie EZK)
	Accountable	Ontwikkeling & Beheer (Afdelingsmanager/kwartiermaker)
	Supportive	Medewerkers in de lijn.
	Consulted	Bestuurlijke en Juridische Zaken en schadeafhandeling (BJZS), (Privacy Officer), Ontwikkeling & Beheer (Functionaris Gegevensbescherming)
	Informed	Bestuur en Management van het IMG
Waarom:	AP (Autoriteit Persoonsgegevens) richtlijnen, Procedure meldplicht datalekken-Ministerie van Economische Zaken	
Risico's en beheersmaatregelen:	<ul style="list-style-type: none"> Niet tijdig melden van een datalek kan gevolgen hebben voor de rechten en vrijheden van natuurlijke personen Grote datalek onbekend Verlies van controle over de persoonsgegevens van betrokkenen 	<ul style="list-style-type: none"> Onderliggende proces/procedure datalek melden binnen de organisatie uitrollen. Bewustwording creëren op het gebied van datalekken.
Vrije tekst/opm.:		



Figur 1 Processchema

1.1. Melden datalek bij Privacy Officer

Wie:	Melder
Input:	Een melding van (vermoeden van) een datalek
Wat:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> • Ontvangt van melder een e-mail in de mailbox met een omschrijving van het datalek (zie Procedure datalekken – paragraaf 7.1 stap 1). <p>De mogelijke interne melders zijn:</p> <ul style="list-style-type: none"> • medewerkers; • managers; • aanvragers; <p>Buitenbeschouwing zijn gehouden meldingen van datalekken bij ketenpartners van IMG. In verwerkerovereenkomsten met deze partijen zijn afspraken gemaakt over het onderling waarschuwen bij een datalek of dreiging daarvan.</p>
Output:	Bevestigingsmail voor het melden van het datalek ter registratie voor (interne) melders.
Werkinstructie: (optioneel)	Memo datalekken in de map 5.1.2.h [REDACTED]
Wanneer:	Direct na het ontdekken van een (vermoedelijk) datalek dit te melden. Zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur nadat er kennis van het datalek is genomen.
Vrije tekst/opm.:	

1.2. Onderzoeken en beoordelen datalek

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	Onderzoeken en beoordelen (mogelijk) gemelde datalek
Wat:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> • Registreert (mogelijk) gemelde datalek; • Onderzoekt en beoordeelt of het gaat om inbreuk op beveiliging van persoonsgegevens van IMG; • Informeert de FG over het datalek. • Stelt vast of het gemelde incident voldoet aan de criteria van een datalek; • Stelt vast wie welke rol heeft (verwerker, verantwoordelijke, medeverantwoordelijke) en wie de meldingsplicht heeft; • Onderzoekt om welke gegevens het gaat; • Stelt vast wat de impact kan zijn voor de personen van wie de gegevens zijn gelekt; • Stelt vast wat de impact kan zijn voor het ministerie; • Stelt vast of het datalek aan AP gemeld moet worden. Beslist of een vrijwillige melding wordt gedaan; • Verzamelt gegevens om melding te kunnen doen bij AP; • Stelt vast of het datalek aan de betrokkenen (aanvragers, medewerkers) moet worden gemeld van wie de gegevens zijn gelekt en stelt vast hoe dat moet gaan gebeuren. Bij een datalek met medewerkersgegevens informeert Privacy Officer in principe ook de getroffen medewerkers, ook in situaties dat dit niet wettelijk verplicht is.
Output:	<ul style="list-style-type: none"> • Mail aan FG over gemelde datalek • Ingevuld datalek formulier inclusief advies van de FG • Uitvoeren stakeholderanalyse bij datalek met DRT (Datalek Response Team)

Werkinstructie: (optioneel)	Stakeholderanalyse stappenplan (RVO)-> IMG
Wanneer:	Zonder onredelijke vertraging, maar binnen 72 uur nadat er kennis van het datalek is genomen (art. 33 lid 1 AVG).
Vrije tekst/opm.:	

1.3. Advies vragen FG

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	Onderzoeken en beoordelen gemelde (mogelijk) datalek
Wat:	De Privacy Officer: <ul style="list-style-type: none"> Vraagt advies aan de Functionaris Persoonsgegevens (FG) bij het beoordelen en onderzoeken van het datalek.
Output:	Ingevuld datalek formulier
Werkinstructie: (optioneel)	
Wanneer:	Zonder onredelijke vertraging, maar binnen 72 uur nadat er kennis van het datalek is genomen.
Vrije tekst/opm.:	

1.4. Datalek alleen bij IMG?

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	Onderzoeken en beoordelen gemelde (mogelijk) datalek
Wat:	De Privacy Officer: <ul style="list-style-type: none"> Beoordeelt of het gaat om inbreuk op beveiliging van persoonsgegevens van IMG; Beoordeelt of het gaat om inbreuk op beveiliging van persoonsgegevens van IMG en ander departement/ministerie.
Output:	Betreft datalek impact ook bij departement/ministerie, ga naar: Ook bij ander departement/ministerie Betreft allen IMG, ga naar: Melden datalek bij AP (indien nodig)
Werkinstructie: (optioneel)	Procedure meldplicht datalekken ministerie EZK (Bij gezamenlijk datalek) Procedure Datalekken IMG
Wanneer:	Zonder onredelijke vertraging, maar binnen 72 uur nadat er kennis van het datalek is genomen.
Vrije tekst/opm.:	

1.5. Ook bij ander departement/ministerie

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	Intern gemelde (mogelijk) datalek
Wat:	De Privacy Officer: <ul style="list-style-type: none"> Concludeert dat ook een ander departement/ministerie betrokken is/zijn bij het datalek; Meldt het incident bij Datalek Reactie Team- Kerndepartement aan (DRT-Kernteam), Ministerie EZK; Stuurt een e-mail naar: 5.1.2.1(contactgegevens) of belt 5.1.2.1 (contactgegevens).
Output:	
Werkinstructie: (optioneel)	Procedure meldplicht datalekken Ministerie EZK
Wanneer:	Zonder onredelijke vertraging, maar binnen 72 uur nadat er kennis van het datalek is genomen.

Vrije tekst/opm.:	Nadat het datalek is gemeld bij Datalek Reactie Team- Kerndepartement onderzoekt en beoordeelt het DRT team de melding en gaat na of de melding gemeld moet worden aan Autoriteit Persoonsgegevens (AP). Dit in i.s.m. de Privacy Officer.
-------------------	--

1.6. Melden datalek bij AP (indien nodig)

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	Beoordeelde datalek met advies van FG of DRT.
Wat:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> Bepaalt na advies van de FG of het datalek wordt gemeld bij de Autoriteit Persoonsgegevens (AP). <p>De FG doet de melding aan de AP. Dit gebeurt via een webformulier (https://datalekken.autoriteitpersoonsgegevens.nl) op de website van AP. Het DRT ondersteunt bij het doen van deze melding in afstemming met andere partijen.</p> <p>Deze melding moet plaatsvinden binnen 72 uur na het ontdekken van het datalek. Eventueel kan een voorlopige melding worden gedaan die daarna wordt aangevuld of wordt teruggetrokken.</p>
Output:	
Werkinstructie: (optioneel)	Procedure Datalekken IMG
Wanneer:	Zonder onredelijke vertraging, maar binnen 72 uur nadat er kennis van het datalek is genomen.
Vrije tekst/opm.:	

1.7. Melden datalek bij betrokkenen (indien nodig)

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	
Wat:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> Beoordeelt de impact van het datalek, en op basis van het aantal personen die geraakt zijn wordt de wijze van communicatie vastgesteld. Betreft het alleen medewerkers, dan kan de manager de medewerkers op de hoogte brengen. Maar betreft het aanvragers, dan kan gekozen worden voor een e-mail, website of callcentre.
Output:	Bij een grootschalig datalek kan ook gebruik worden gemaakt van een incidententafel, website en helpdesk.
Werkinstructie: (optioneel)	Procedure Datalekken IMG
Wanneer:	Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee (art. 34 lid 1 AVG Betrokkenen).
Vrije tekst/opm.:	

1.8. Afstemmen op afhandeling

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	
Wat:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> Heeft nauwe contacten met partijen en functionarissen die een rol spelen bij het afhandelen van het incident.

	<p>Deze kunnen zijn:</p> <ul style="list-style-type: none"> • ICT en security, voor inzicht op oorzaak van incident en genomen maatregelen. Ook zal mogelijk IT forensisch onderzoek noodzakelijk zijn om vast te stellen welke persoonsgegevens gecompromitteerd zijn; • Integriteit, indien EZ-medewerkers een rol hebben bij het veroorzaken van het datalek; • De afdelingen/directies die te maken hebben met de verstoring van het bedrijfsproces; • Interne en externe communicatie; Zie Art. 4.1 Procedure Datalekken IMG • Juridische zaken.
Output:	
Werkinstructie: (optioneel)	Procedure Datalekken IMG
Wanneer:	
Vrije tekst/opm.:	

1.9 Nazorg datalek

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	
Wat:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> • Bepaalt de wijze van nazorg, deze is afhankelijk van de grootschaligheid of type datalek. Noodzakelijk is het uitvoeren van een contactpunt voor het geven van extra informatie, van nader handelingsperspectief om de schade te verkleinen of actieve ondersteuning om de schade te beperken.
Output:	
Werkinstructie: (optioneel)	Procedure Datalekken IMG
Wanneer:	
Vrije tekst/opm.:	

1.10 Evalueren afhandeling datalek

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	<p>De Privacy Officer:</p> <ul style="list-style-type: none"> • Evalueert samen met de FG de wijze van beoordeling van het signaal en het afhandelen daarvan na de afhandeling van een datalek.
Wat:	
Output:	
Werkinstructie: (optioneel)	Procedure Datalekken IMG
Wanneer:	
Vrije tekst/opm.:	

1.11 Rapporteren

Wie:	Ontwikkeling & Beheer (Privacy Officer)
Input:	
Wat:	De Privacy Officer:

	<ul style="list-style-type: none">• Rapporteert per kwartaal aan het MT, de volgende zaken worden gerapporteerd; het aantal datalekken, de impact, de nazorg enz.
Output:	Finale rapportage datalekken
Werkinstructie: (optioneel)	Procedure Datalekken IMG
Wanneer:	
Vrije tekst/opm.:	



Procedure Datalekken

Instituut Mijnbouwschade Groningen (Het Instituut)

Eigenaar: 5.1.2.e

Datum : 29 september 2023

Versie : D 1.1

Status : Definitief

Colofon

Procedure	Datalekken
Contactpersoon	5.1.2.e [redacted] privacy@schadedoormijnbouw.nl Instituut Mijnbouwschade Groningen Cascadeplein 10 9726 AD Groningen
Auteurs	5.1.2.e en 5.1.2.e
Versie	D 1.0
Bijlage(n)	5

Versie	Datum	Door	Wijzigingen
0.1	23-02-2022	5.1.2.e	Concept opgesteld
0.2	20-04-2022	5.1.2.e	Opzet veranderd
0.3	17 augustus 2023	5.1.2.e	Concept herzien
0.4	17 augustus 2023	5.1.2.e	Feedback verwerkt
0.5	22 augustus 2023	5.1.2.e	Feedback verwerkt
1.0	31 augustus 2023	5.1.2.e	Definitief gemaakt
1.1	29 september 2023	5.1.2.e [redacted]	Vastgesteld door 5.1.2.e [redacted].

Inhoudsopgave

1.	Inleiding	4
1.1	Leeswijzer.....	4
2.	Wat is een datalek?	5
2.1.	Definitie	5
2.2.	Soorten datalekken	5
2.3.	(Mogelijke) gevolgen datalek	5
3.	Datalekken.....	6
3.1.	Intern datalek.....	6
3.2.	Extern datalek	8
3.3.	Grootschalig datalek	8
4.	Melding aan de toezichhoudende autoriteit	11
4.1.	Wanneer moet een datalek gemeld worden aan de toezichhoudende autoriteit?	11
4.2.	Termijn	11
4.3.	Waar melden?.....	11
5.	Melding aan betrokkenen.....	12
5.1.	Wanneer en wat melden aan betrokkenen?	12
5.2.	Uitzonderingen	12
6.	Beoordeling van het risico.....	13
7.	Verantwoordingsplicht en registratie.....	14
	Bijlagen	15
1.	Beslisboom datalek melden	15
2.	Formulier datalekken en incidenten	16
3.	Procesbeschrijving	16
4.	Template brief melding betrokkene	17
5.	Evaluatieformulier Datalekken	19

1. Inleiding

In de Algemene verordening gegevensbescherming (hierna: AVG) is een verplichting opgenomen om een inbreuk in verband met persoonsgegevens (ook wel datalek genoemd) te melden aan de toezichthouder, de Autoriteit Persoonsgegevens (hierna: de AP), en, in gevallen waarbij sprake is van een hoog risico, ook aan de betrokkenen (de personen op wie de gegevens die zijn gelekt betrekking hebben; bijvoorbeeld aanvragers of medewerkers van het Instituut Mijnbouwschade Groningen, hierna: het Instituut).¹ De AVG stelt strenge eisen aan de omgang met datalekken. Organisaties moeten alle datalekken registreren. Aan de hand van deze documentatie kan de toezichthoudende autoriteit controleren of de organisatie zijn verplichtingen omtrent de omgang met datalekken is nagekomen.

In deze procedure wordt omschreven op welke manier Instituut omgaat met (eventuele) datalekken. In de procedure is vastgelegd hoe en naar wie de meldingen intern doorgezet dienen te worden, wie intern verantwoordelijk is en voor welke melding, hoe de melding aan de toezichthouder wordt gedaan en hoe de betrokkenen eventueel geïnformeerd moeten worden. **Deze procedure is een afgeleide van het proces melden datalekken D1.0 (zie bijlage 3)**. Deze procedure is eveneens gebaseerd op de 'Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens' van de Artikel 29-werkgroep..

In onderstaande afbeelding wordt kort samengevat of en wanneer er een melding gedaan dient te worden.



Mochten toekomstige (wettelijke) wijzigingen/veranderingen het aanpassen van dit document noodzakelijk maken, dan zal de hiervoor aangewezen persoon binnen het Instituut aanpassing doorvoeren en het versienummer updaten.

1.1 Leeswijzer

In hoofdstuk 2 wordt uiteengezet wat een datalek is. In hoofdstuk 3 wordt de procedure voor het afhandelen van een datalek stapsgewijs uitgelegd. In de hoofdstukken daarna worden stappen uit

¹ In Nederland bestaat deze meldplicht datalekken al sinds 1 januari 2016.

deze procedure nader toegelicht. In hoofdstuk 4 en 5 wordt toegelicht hoe een melding moet worden gedaan bij de toezichthoudende autoriteit respectievelijk de betrokkene. Hoofdstuk 6 zet uiteen hoe een risico van een datalek wordt beoordeeld. Tot slot wordt er in hoofdstuk 7 toegelicht hoe een datalek dient te worden geregistreerd.

2. Wat is een datalek?

2.1. Definitie

In de AVG wordt een datalek als volgt gedefinieerd:

“Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.”²

Hierbij wordt met de vernietiging van persoonsgegevens bedoeld dat de gegevens niet langer bestaan en de beschadiging van gegevens houdt in dat de persoonsgegevens gewijzigd of niet langer volledig zijn. Bij het verlies van persoonsgegevens heeft de verwerkingsverantwoordelijke, zoals het Instituut, niet langer controle over of toegang tot de gegevens. Tenslotte heeft de ongeoorloofde of onrechtmatige verwerking van persoonsgegevens betrekking op het verstrekken van persoonsgegevens aan onbevoegden.

2.2. Soorten datalekken

Er zijn drie verschillende soorten datalekken:

- Inbreuk op de vertrouwelijkheid: wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van of toegang tot persoonsgegevens.
- Inbreuk op de integriteit: wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.
- Inbreuk op de beschikbaarheid: wanneer er sprake is van onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van persoonsgegevens.

Afhankelijk van de omstandigheden kan een datalek in verschillende categorieën vallen. Voorbeelden van datalekken zijn:

- een verloren USB-stick met niet-versleutelde persoonsgegevens;
- een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- een besmetting met ransomware waardoor persoonsgegevens ontoegankelijk zijn gemaakt;
- een brand in een datacentrum;
- het doorsturen van gegevens naar de verkeerde persoon; of
- het verzenden van een e-mail met de e-mailadressen in de CC in plaats van de BCC.

2.3. (Mogelijke) gevolgen datalek

Een datalek kan erg vervelend zijn voor de betrokkene(n). Het kan leiden tot lichamelijke, materiële en immateriële schade. In de AVG worden voorbeelden gegeven van eventuele negatieve gevolgen voor betrokkenen, namelijk:

- het verlies van controle over hun persoonsgegevens;
- het niet kunnen uitoefenen van hun rechten (zoals wissing of rectificatie);
- discriminatie;
- identiteitsdiefstal of -fraude;
- financiële verliezen;
- ongedaan maken van pseudonimisering;
- reputatieschade;
- of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de persoon in kwestie

Of deze schade zich daadwerkelijk voordoet is niet relevant voor de vraag of er sprake is van een datalek.³

² Zie artikel 4 onder 12 AVG.

³ Zie overweging 85 AVG.

Daarom is in de AVG vastgelegd dat de verwerkingsverantwoordelijke verplicht is een datalek aan de bevoegde toezichthoudende autoriteit te melden, tenzij het onwaarschijnlijk is dat het datalek zal leiden tot een risico voor de rechten en vrijheden van betrokkenen, zie hoofdstuk 3.⁴ Indien de waarschijnlijkheid van dit risico hoog is, zal het datalek ook aan de betrokkenen gemeld moeten worden, *zie hoofdstukken 5 en 6*.⁵

3. Datalekken

Een datalek kan zowel bij het Instituut binnen de eigen organisatie als bij een door het Instituut ingeschakelde verwerker (denk hierbij aan ICT-leverancier, de hosting provider of een ingeschakeld deskundige partij) plaatsvinden. Wanneer een datalek zich voordoet, zal vastgesteld moeten worden waar het datalek zich heeft voorgedaan en hoe dit datalek uiteindelijk bij de toezichthouder en eventueel bij de betrokkenen gemeld zal worden. Het vaststellen van een datalek zal in eerste instantie de taak zijn van de Privacy Officer en hij doet dit in samenspraak met de Security Officer. De Functionaris Gegevensbescherming (hierna: de FG) zal het contact met de toezichthouder en eventuele betrokkenen op zich nemen. Zij zijn via onderstaande contactgegevens te bereiken:

- Privacy Officer
Email: privacy@schadedoormijnbouw.nl
- Functionaris Gegevensbescherming
:
Email: FG@schadedoormijnbouw.nl
- Security Officer
Email: 5.1.2.1 (contactgegevens) [@Schadedoormijnbouw.nl](mailto: @Schadedoormijnbouw.nl)

Uiteraard is het belangrijk dat alle betrokken personen, dus zowel het personeel van het Instituut als het personeel bij de ingeschakelde derden, een datalek kunnen identificeren. Het creëren van bewustzijn bij het personeel van het Instituut is dan ook van groot belang. Hier zal dan ook voldoende aandacht aan worden geschonken. In het geval dat een incident wordt ontdekt dan zal de ontdekker dit in ieder geval onverwijld moeten melden bij de Privacy Officer en/of de FG.

3.1. Intern datalek

Wanneer er binnen het Instituut een datalek plaatsvindt zal iedereen moeten weten hoe er gehandeld dient te worden zodat de melding tijdig de juiste personen, de toezichthouder en de betrokkenen bereikt.

De algemene procedure omtrent het afhandelen van een datalek bestaat uit een aantal stappen die doorlopen worden.

Stappen:

1. Stap 1: Melden datalek bij Privacy Officer en Security Officer

De ontdekker en/ of melder van het datalek meldt bij ontdekking van het datalek dit zo spoedig mogelijk bij de Privacy Officer. Ook bij twijfel neemt de ontdekker /melder contact op met de Privacy Officer. Alle medewerking dient te worden verleend aan de Privacy Officer en daarbij dient de melder zo snel en goed mogelijk antwoord te geven op de volgende vragen:

- Wat is er gebeurd (omschrijving van het incident);
- Is dit een mogelijke fout vanuit een handeling die past bij het normaal uitvoeren van werkzaamheden, of is er vermoedelijk sprake van opzet, eventueel van buitenaf;
- Is het datalek veroorzaakt door een menselijke handeling of technische fout (bijvoorbeeld koppeling tussen dossiers in twee systemen door een programeerfout);

⁴ Zie artikel 33 AVG.

⁵ Zie artikel 34 AVG.

- Wanneer is het gebeurd (Datum en tijdstip);
- Wanneer is het ontdekt;
- Welke systemen zijn bij dit datalek betrokken;
- Zijn er tussentijdse maatregelen getroffen om het datalek te dichten? Zo ja, welke;
- Wat voor gegevens (registers) zijn gelekt ;
- Zijn de gegevens versleuteld, en zo ja hoe ;
- Konden de gegevens op afstand worden gewist of ontoegankelijk gemaakt, en zo ja is dat gebeurd;
- Wat zijn de mogelijke gevolgen voor de betrokkenen;
- Welke groep(en) personen is/zijn hierdoor getroffen;
- Hoeveel personen zijn hierdoor (bij benadering) getroffen;
- Zijn er ook gegevens van personen in andere EU-landen getroffen door het datalek;
- Konden er al technische en/of organisatorische maatregelen worden getroffen naar aanleiding van het incident ?

Bovenstaande gegevens zijn van belang om het datalek te beoordelen door de Privacy Officer bij stap 2 (zie ook hoofdstuk 7 voor een nadere toelichting). Daarnaast dient de Security Officer ook bij de melding te worden geraadpleegd. De Security Officer kan dan direct de desbetreffende proces- of systeemeigenaar adviseren om tussentijdse maatregelen te nemen om het datalek op technisch vlak te dichten. Zo kan een verdere inbreuk dan wel schade worden voorkomen. Indien op basis van bovenstaande informatie het vermoeden van een integriteitskwestie bestaat, zal Bureau Bijzonder Onderzoek van het Instituut worden ingeschakeld (zie stap 8).

De melder heeft altijd de mogelijkheid om rechtstreeks bij de FG een melding te doen. De FG zal het verdere verloop van stappen 1 en 2 afstemmen met de Privacy Officer en Security Officer.

2. *Stap 2: Onderzoeken en beoordelen datalek*

De Privacy Officer onderzoekt op basis van bovenstaande gegevens of er sprake is van een datalek en beoordeelt het risico van het lek conform het proces melden datalekken (bijlage 3). Tevens registreert de Privacy Officer het datalek in het datalekkenregister (zie hoofdstuk 7). De Privacy Officer bewaart alle records die voor de beoordeling van het datalek van belang zijn geweest. De verantwoordelijke van de afdeling van de ontdekker/melder van het datalek, alsmede de ontdekker/melder zelf en degene die belast zijn met het nemen van technische en organisatorische maatregelen binnen het Instituut blijven 24 uur (afhankelijk van de omvang en ernst van het datalek en indien mogelijk) beschikbaar na melding, zodat de Privacy Officer en Security Officer alle maatregelen kunnen nemen die voortvloeien uit het datalek.

3. *Stap 3: Advies vragen FG*

De Privacy Officer meldt het lek bij de FG. De FG beoordeelt vervolgens of er sprake is van een (hoog) risico voor de rechten en vrijheden van betrokkenen en adviseert het privacyteam hierover. De FG meldt het lek zelf bij de AP (zie stap 6) dan wel betrokkene (zie stap 7) of geeft het privacyteam hiertoe de opdracht.

4. *Stap 4: Datalek alleen bij het Instituut?*

Indien het alleen een datalek bij het Instituut betreft, dan wordt er op basis van het advies van de FG wel of geen melding gemaakt bij de AP (zie stap 6).

5. *Stap 5: Ook bij ander departement/ministerie*

Indien er andere departementen zijn betrokken bij het datalek, dan meldt de Privacy Officer of de FG het datalek conform het proces melden datalekken bij de verantwoordelijke binnen het ministerie zonder onredelijke vertraging.

6. *Stap 6: Melden datalek aan AP (indien nodig)?*

De FG meldt in eerste instantie het lek bij de AP, zo snel mogelijk maar uiterlijk binnen de maximale wettelijke termijn na ontdekking van het datalek. Is de FG niet beschikbaar, dan doet de Privacy Officer een voorlopige melding bij de AP, eveneens binnen diezelfde termijn. De melding gaat gepaard met de beantwoording van de vragen zoals bedoeld in stap 1. In hoofdstuk 4 wordt dit proces nader uiteengezet.

7. *Stap 7: Melden datalek bij betrokkenen (indien nodig)*

De FG meldt een datalek bij betrokkenen indien het datalek wordt ingeschat als een hoog risico voor de rechten of vrijheden van de betrokkenen. De FG doet dit door middel van een officiële brief die wordt ondertekend door de portefeuillehouder AVG van het bestuur van het Instituut (zie bijlage 4). Het verzenden van de brief en overige administratieve afhandeling kan ook worden belegd bij de Privacy Officer. In de hoofdstukken 5 en 6 wordt dit proces nader uiteengezet.

8. Stap 8: Afstemmen op afhandeling

De Privacy Officer blijft in contact met de Security Officer en andere functionarissen die betrokken zijn bij de afhandeling van het datalek om het datalek zorgvuldig af te handelen. 5.1.2.i



9. Stap 9: Nazorg datalek

De Privacy Officer bepaalt de wijze van nazorg. De nazorg is afhankelijk van de grootschaligheid of het type datalek. Voor grootschalige datalekken wordt de procedure onder paragraaf 3.3. gevolgd. De Privacy Officer bepaalt in samenspraak met de Security Officer en de overige functionarissen de juiste nazorg voor het datalek. De Privacy Officer koppelt de nazorg van het datalek terug aan de desbetreffende afdeling door middel van het ingevulde datalekkenformulier (zie bijlage 2).

10. Stap 10: Evalueren afhandeling datalek

De Privacy Officer evalueert samen met de FG de wijze van beoordeling van het signaal en het afhandelen daarvan. Zij formuleren samen met de Security Officer en andere functionarissen eventuele beheersingsmaatregelen om toekomstige datalekken te voorkomen en leggen dit voor aan management d.m.v. een evaluatieformulier zoals bedoeld in bijlage 5.

11. Stap 11: Rapporteren

De Privacy Officer rapporteert per kwartaal samen met de Security Officer de volgende zaken aan het management van het Instituut: het aantal datalekken; de impact en de nazorg; enzovoorts. Bij impactvolle/ernstige datalekken stellen zij samen beheersingsmaatregelen voor aan het management. Het management neemt de uiteindelijke beslissingen om de maatregelen in te voeren.

3.2. Extern datalek

Een datalek kan ook buiten (extern) het Instituut plaatsvinden, bijvoorbeeld bij verwerkers. Onder de AVG zijn verwerkers verplicht om zodra zij kennis hebben genomen van een inbreuk deze zonder onredelijke vertraging, binnen 24 uur, aan de verantwoordelijke te melden..

Door middel van verwerkersovereenkomsten zijn met deze derde partijen contractuele verplichtingen aangegaan, die verplichten om het datalek binnen bovengenoemde termijn te melden. Elke externe partij heeft in de verwerkersovereenkomst een vaste contactpersoon aangegeven, veelal de FG, om meldingen betreffende datalekken zo snel en gestroomlijnd mogelijk te laten verlopen. Contactgegevens van de Privacy Officer en FG van het Instituut staan tevens vermeld in de verwerkersovereenkomst.

In het geval dat het Instituut van buitenaf bericht krijgt over een (vermeende) inbreuk op de persoonsgegevens waar het Instituut voor verantwoordelijk is, dan dienen de bovengenoemde stappen (paragraaf 3.1) te worden gevolgd.

3.3. Grootschalig datalek

Het kan voorkomen dat er een datalek is door een systeem/ applicatie met veel persoonsgegevens of op een datalek bij de IT-organisatie waar meerdere systemen of applicaties met persoonsgegevens draaien. Hiervan heeft de AP bepaald dat er bij een dergelijke lek een aanmerkelijke risico bestaat op het aantasten van de rechten en vrijheden van een groot aantal betrokkenen. In een dergelijk

6
5.1.2.h
P

geval dient de FG al dan niet in samenwerking met anderen dit datalek onverwijld te melden aan al die betrokkenen.

Bij het melden van het datalek aan de betrokkenen kan het voorkomen dat de contactgegevens van de betrokkene(n) niet meer actueel zijn. Indien dit het geval is dan dient het Instituut volgens de AVG een redelijke inspanning te verrichten om alle betrokkenen te informeren. Indien de juiste contactgegevens van betrokkenen moeilijk te achterhalen zijn, dan volstaat het kunnen aantonen van die redelijke inspanning. Let op: dit gegeven dient wel te worden geregistreerd in het datalek register!

In het geval dat er sprake is van een grootschalige datalek bij het Instituut dan dienen de volgende stappen te worden ondernomen:

Stap 1: Voorbereiding

Om de situatie effectief en efficiënt aan te pakken dienen meerdere organisatieonderdelen mee te denken aan de afhandeling van het datalek. Hierbij kan de FG een incidententafel organiseren. Deze tafel zal in ieder geval de volgende leden hebben:

- manager van de beheersorganisatie die verantwoordelijk is voor het beheer van de systemen/applicaties waarmee de desbetreffende verwerking van persoonsgegevens plaatsvindt en daarmee ook verantwoordelijk is voor het treffen van adequate beveiligingsmaatregelen op het desbetreffende systeem/applicatie;
- manager/leidinggevende die bij het Instituut verantwoordelijk is voor de uitvoering van het bedrijfsproces dat dit systeem/applicatie ondersteunt;
- leidinggevende/manager afdeling communicatie;
- materiedeskundigen, bijvoorbeeld Functioneel Beheer⁷;
- een notulist (zie stap 7);
- bedrijfsjurist c.q. huisadvocaat van het Instituut;
- Privacy Officer, Security Officer, CISO;
- FG

De FG communiceert met het management en het bestuur over het inroepen van een incidententafel en houdt beiden op de hoogte van het proces. Tegelijkertijd zal de AP op de hoogte worden gebracht van het datalek en zal de FG contact houden met de AP.

Stap 2: Uitvoering

Incidententafel

- De FG, al dan niet in samenwerking met anderen, brengt in kaart welke gegevens van welke betrokkenen zijn gelekt;
- welke gevolgen en risico's een dergelijk lek kan hebben voor de betrokkene(n);
- of en zo ja, hoe deze gevolgen en risico's zich daadwerkelijk hebben voltrokken/ alsnog kunnen voltrekken (root cause analyse);
- welke maatregelen de organisatie al heeft genomen, alsook de te nemen maatregelen om deze gevolgen en risico's te voorkomen of verminderen (het isoleren van het probleem);
- met welke personen de betrokkenen contact kunnen opnemen voor meer informatie;
- hoeveel tijd, geld, middelen en kwaliteit noodzakelijk is om de betrokkenen volledig, adequaat en juist te informeren en te ondersteunen.

NB. De beslissing over de hoeveelheid tijd, geld, middelen en kwaliteit worden ingezet om verzachtende maatregelen te treffen en betrokkenen te informeren worden op bestuursniveau van het Instituut genomen. Echter wordt het bestuur hierin geadviseerd door de FG. De FG kan het advies baseren op de gesprekken die zijn gevoerd met leden tijdens de incidententafel.

Stap 3: Informatie aan betrokkenen

Het Instituut informeert betrokkenen per brief en/of e-mail: hiervoor zijn de NAW-gegevens en/of de mailadressen van betrokkenen nodig. De correspondentie met de betrokkenen omvat in ieder geval de volgende informatie:

Buiten reikwijdte

- welke gegevens zijn gelekt;
- de oorzaak/ oorzaken van het lek;
- de mogelijke gevolgen en risico's van het lek voor de betrokkenen;
- welke maatregelen er zijn getroffen om deze gevolgen te voorkomen/ mitigeren;
- welke maatregelen de betrokkenen eventueel zelf kan nemen om de gevolgen en risico's te verminderen en hoe ze dit het beste kunnen aanpakken;
- verwijzen naar een website/ helpdesk/ FG voor nadere informatie;
- of en zo ja, welke informatie, hoe en wanneer nog volgt;
- of en zo ja, welke hulp of schadevergoeding Het Instituut aanbiedt, gegeven de aard en ernst van de gelekte gegevens en de daaruit voortvloeiende schade voor betrokkenen.

De FG en management kunnen ervoor kiezen om de betrokkenen niet persoonlijk aan te schrijven maar grootschalige communicatiemiddelen in te zetten. In dat geval zal bovenstaande informatie, zonder dat dit invloed heeft op de afhandeling van het datalek of een risico biedt voor het Instituut en/of betrokkenen, op de website van het Instituut worden gepubliceerd. Indien er sprake is van een zeer ernstig lek, kan management ervoor kiezen om de leiding over te nemen van de FG met betrekking tot het grootschalige datalek. Zie hiervoor tevens stap 5.

Stap 4: Inrichten van helpdesk

Bij een grootschalig datalek is het onwaarschijnlijk dat de FG alleen alle vragen van betrokkenen kan beantwoorden. In een dergelijk geval is het Instituut gebaat om een helpdesk in te richten. Hierbij is het belangrijk dat:

- Het Instituut een helpdesk (direct telefoonnummer/mailbox) inricht die beschikbaar/ open is gedurende werkdagen en kantooruren waarbij betrokkenen contact kunnen opnemen voor aanvullende informatie omtrent het datalek;
 - de medewerkers van de helpdesk in ieder geval in staat zijn om algemene informatie te verstrekken aan betrokkenen, deze gegevens bevatten in ieder geval de bij 'informatie aan betrokkenen' genoemde punten;
 - indien mogelijk de medewerkers van de helpdesk, al dan niet in samenwerking met de FG, in staat zijn om de betrokkenen ook van specifieke informatie te verstrekken over hun specifieke persoonlijke situatie naar aanleiding van het ontstane datalek.

Stap 5: Vermelden website

Bij grootschalige datalekken kan het Instituut gebruikmaken van de openbare website waarbij op de homepage een directe link wordt vermeld waarbij het Instituut de betrokkenen in staat stelt om algemene informatie te raadplegen. Deze informatie bevat in ieder geval de bij 'informatie aan betrokkenen' (stap 3) genoemde punten. Indien het lek als zeer ernstig wordt ingeschat, legt management de leiding over externe communicatie neer bij de afdeling Communicatie. De FG wordt wel geraadpleegd met betrekking tot de externe communicatie.

NB. Indien nodig worden de betrokkenen tussentijds geïnformeerd over de voortgang van de afwikkeling van het datalek, met inbegrip van de bij 'informatie aan betrokkenen' genoemde punten.

Stap 6: nazorg en evaluatietafel

De FG beoordeelt of het datalek is gedicht en of alle noodzakelijke maatregelen zijn getroffen om het risico te verminderen op een herhaling van eenzelfde of vergelijkbaar datalek. Ook beoordeelt de FG of alle noodzakelijke maatregelen zijn getroffen die volgen uit of verband houden met de meldplicht aan de betrokkenen. Via de notulen die de notulist inzake heeft de incidententafel heeft opgesteld, organiseert de FG tevens een evaluatietafel. Deze tafel bestaat uit dezelfde leden als de incidententafel en Interne Controle. Interne Controle ziet er op toe dat de (zelf)evaluatie correct verloopt. Deze evaluatietafel behandelt de volgende vragen:

- Wat is er precies gebeurd en op welke tijdstippen vond dit plaats;
- Hoe goed presteerde medewerkers en het management tijdens het incident;
- Is de gedocumenteerde procedure gevolgd en was deze adequaat;
- Welke informatie had sneller beschikbaar moeten zijn;
- Zijn er stappen of acties ondernomen die het herstel zouden kunnen hebben belemmerd;
- Wat zouden de medewerkers en het management een volgende keer anders doen wanneer een gelijksoortig incident plaatsvindt;
- Hoe zou het delen van informatie met betrokkenen, organisaties, overheidsinstanties en/of overige derde partijen beter kunnen;
- Welke correctieve acties kunnen gelijksoortige incidenten in de toekomst voorkomen;

- Op welke voortekenen of indicatoren moet in de toekomst worden gelet om soortgelijke incidenten op te sporen;
- Welke aanvullende instrumenten of middelen zijn nodig om toekomstige incidenten op te sporen, te analyseren en te beperken?

Uit deze evaluatie volgt een aanbeveling in de vorm van een rapportage. Een aanbeveling kan zijn om mogelijke gerechtelijke stappen te nemen tegen de veroorzaker van het datalek (bijvoorbeeld bij het verwijtbaar handelen van een verwerker).

Verder beoordeelt de FG of dit datalek en het oplossen van de impact daarvan kan worden afgewikkeld. Indien dit mogelijk is dan beslist de FG tot afronding van het incident, tot ontbinding van de incidententafel en evaluatietafel, tot het beëindigen van de helpdesk en tot het deactiveren van de informatiepagina op de externe website van het Instituut in samenspraak met management.

De FG stuurt de betrokkenen per brief of per mail een afloopbericht over de definitieve afwikkeling van het datalek, waaronder de getroffen maatregelen om het lek te dichten en de gevolgen en risico's voor de betrokkenen te voorkomen of mitigeren. Indien van toepassing; wordt in de brief informatie gegeven over de ondersteuning en/ of vergoeding van de schade voor betrokkenen.

4. Melding aan de toezichhoudende autoriteit

4.1. Wanneer moet een datalek gemeld worden aan de toezichhoudende autoriteit?

Op het moment dat er sprake is van een datalek zoals omschreven in hoofdstuk 2, dan is het aan het Instituut om per datalek te beoordelen of het datalek aan de toezichhouder gemeld moet worden. In de AVG is bepaald dat een datalek aan de toezichhouder gemeld moet worden indien de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Normaliter komt deze beoordeling toe aan de verwerkingsverantwoordelijke van deze persoonsgegevens. Indien het Instituut als verwerkingsverantwoordelijke kan worden gezien dient het Instituut zelf een melding te maken bij de toezichhouder. Wanneer het Instituut optreedt als verwerker zal zij het datalek bij de verwerkingsverantwoordelijke moeten melden.

Voor de meldplicht van een datalek aan de toezichhouder, moet er dus sprake zijn van een risico voor de rechten en vrijheden van de betrokkenen. In hoofdstuk 6 wordt uiteengezet waarmee rekening gehouden moet worden bij het beoordelen van het risico.

4.2. Termijn

Het datalek dient door de verwerkingsverantwoordelijke zo snel mogelijk, maar uiterlijk binnen 72 uur nadat hij er kennis van heeft genomen, aan de toezichhoudende autoriteit gemeld te worden. Deze termijn start op het moment dat het Instituut, al dan niet via één van haar (sub)verwerkers, op de hoogte raakt van het datalek.

Datalekken moeten dus binnen 72 uur na ontdekking worden gemeld bij de toezichhouder. Het is mogelijk dat het Instituut binnen deze periode nog niet alle relevante informatie heeft verzameld. In een dergelijk geval is het mogelijk om een voorlopige melding te doen en deze aan te vullen zodra overige informatie beschikbaar is.

Verwerker

Indien het Instituut in de rol van verwerker handelt (dit zal veelal niet het geval zijn) zal de termijn voor het melden van het datalek aan de verwerkingsverantwoordelijke in veel gevallen zijn vastgelegd in de verwerkersovereenkomst. Het Instituut moet de inbreuk in ieder geval zonder onredelijke vertraging aan verwerkingsverantwoordelijke melden.

4.3. Waar melden?

Een melding van een datalek dient via de website van de toezichhoudende autoriteit te worden doorgegeven. In Nederland is dat de website van de AP: <https://datalekken.autoriteitpersoonsgegevens.nl> Bij de melding moet in ieder geval de volgende informatie verstrekt worden:

- De aard van de inbreuk;

- de categorieën en het aantal betrokkenen;
- het soort persoonsgegevens;
- de naam en contactgegevens van de FG of Privacy Officer die de afhandeling op zich neemt;
- de waarschijnlijke gevolgen van de inbreuk;
- de maatregelen die genomen zijn of gaan worden om de gevolgen in te perken.

5. Melding aan betrokkenen

5.1. Wanneer en wat melden aan betrokkenen?

In bepaalde gevallen moet het Instituut de inbreuk niet alleen melden aan de toezichhoudende autoriteit (de AP), maar ook aan de personen die door de inbreuk zijn getroffen (de betrokkenen). Dit is het geval wanneer de inbreuk met persoonsgegevens waarschijnlijk een **hoog** risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De drempel voor het melden aan betrokkenen ligt dus hoger dan die voor het melden aan de toezichhoudende autoriteit. Het staat de FG en Privacy Officer echter vrij om het datalek te melden bij de betrokkenen zonder dat er een hoog risico voor de rechten en vrijheden van betrokkenen bestaat.

Er is sprake van een hoog risico indien de te verwachten gevolgen van het datalek zich met grote waarschijnlijkheid voordoen. Voorbeelden van negatieve gevolgen die zich voor zouden kunnen doen bij een datalek zijn terug te vinden in paragraaf 2.3.

Betrokkenen moeten onverwijld (zo snel mogelijk) over de inbreuk geïnformeerd worden.⁸ De melding moet in duidelijke en eenvoudige taal de volgende informatie bevatten:

- Een omschrijving van de aard van de inbreuk;
- de naam en contactgegevens van de Functionaris Gegevensbescherming of andere persoon die de afhandeling op zich neemt;
- de waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
- de maatregelen die genomen zijn of worden genomen om de inbreuk aan te pakken, waaronder de maatregelen om de gevolgen in te perken; en
- tips over wat mensen zelf kunnen doen om zichzelf te beschermen.

Deze melding wordt gedaan betrokkene middels een brief die wordt opgesteld door de FG en ondertekend door de portefeuillehouder AVG van het bestuur (zie bijlage 4).

5.2. Uitzonderingen

De AVG kent drie uitzonderingen op de meldplicht aan betrokkenen:

1. De organisatie is een financiële onderneming als bedoeld in de Wet op het financieel toezicht;⁹
2. Het Instituut heeft passende technische en organisatorische beschermingsmaatregelen genomen (zoals versleuteling) en deze maatregelen toegepast op de persoonsgegevens waarop het datalek betrekking heeft waardoor de persoonsgegevens onbegrijpelijk zijn voor onbevoegden. Door deze beveiliging is misbruik uit te sluiten;¹⁰
3. Het Instituut heeft direct maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich (waarschijnlijk) niet meer zal voordoen.¹¹

Er kunnen zich ook situaties voordoen waarin de mededeling onevenredig veel inspanning zou vergen. In dat geval hoeven betrokkenen niet individueel geïnformeerd te worden, maar moeten de betrokkenen wel via een openbare mededeling of soortgelijke maatregel doeltreffend worden geïnformeerd.¹²

⁸ Zie overweging 86 AVG.

⁹ Zie artikel 42 42 UAVG.

¹⁰ Zie artikel 34 onder 3(a) AVG.

¹¹ Zie artikel 34 onder 3(b) AVG.

¹² Art. 34 onder 3(c) AVG.

NB: in deze gevallen moet de toezichhoudende autoriteit wel geïnformeerd worden. Aan de hand van deze melding kan de toezichhouder het Instituut instrueren alsnog melding te doen aan de betrokkenen.¹³

6. Beoordeling van het risico

De verplichting om een inbreuk te melden aan de toezichhouder dan wel aan de betrokkenen hangt af van het risico dat met de inbreuk gepaard gaat. Het Instituut zal na kennisneming van een inbreuk het incident onder controle moeten krijgen, maar zal daarnaast ook zo snel mogelijk het risico moeten inschatten dat eruit kan voortvloeien.

Zoals in de vorige hoofdstukken uiteen is gezet moet een inbreuk:

1. gemeld worden aan de toezichhouder indien deze een risico inhoudt voor de rechten en vrijheden van natuurlijke personen; en
2. medegedeeld worden aan betrokkenen indien deze waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen met zich meebrengt.

Bij de beoordeling van de risico's moet door het Instituut rekening gehouden worden met zowel de waarschijnlijkheid als de ernst van het risico voor de rechten en vrijheden van betrokkenen. Aan de hand van de volgende factoren kunnen risico's beoordeeld worden:

1. De aard van de inbreuk (vertrouwelijkheid, integriteit of beschikbaarheid)

Wanneer een personeelsdossier verstrekt wordt aan onbevoegden kan dit andere gevolgen hebben dan wanneer er per ongeluk gegevens uit het personeelsdossier verwijderd zijn.

2. De aard, gevoeligheid en omvang van de persoonsgegevens

Een inbreuk waarbij NAW-gegevens gecompromitteerd zijn levert in de meeste gevallen een minder hoog risico op dan een inbreuk waarbij financiële gegevens gestolen worden. Er zal tevens gekeken moeten worden naar de omvang; gaat het om één persoonsgegeven of om een combinatie van gegevens waardoor er een volledig beeld van de betrokkenen geschetst kan worden? Indien bij een inbreuk bijvoorbeeld gezondheidsgegevens, identiteitsdocumenten en financiële gegevens betrokken zijn zou dit kunnen leiden tot identiteitsdiefstal.

3. Het gemak waarmee personen kunnen worden geïdentificeerd

Indien het voor een onbevoegde gemakkelijk is om specifieke personen te identificeren of de gegevens te koppelen met andere informatie om personen te identificeren zal er eerder sprake zijn van een (hoog) risico. Afhankelijk van de omstandigheden van het geval zal het soms mogelijk zijn om betrokkenen direct of indirect te identificeren.

4. De ernst van gevolgen voor personen

Een datalek kan leiden tot identiteitsdiefstal of -fraude, lichamelijk letsel, psychisch leed, vernedering of reputatieschade. Bij het inschatten van de ernst van de gevolgen dient rekening te worden gehouden met de intenties van de personen waarbij de persoonsgegevens mogelijk terecht zijn gekomen. Deze kunnen onbekend zijn of zelfs kwaadwillig, dit heeft invloed op het potentiële risico. Het risico dat misbruik gemaakt zal worden van gegevens die per ongeluk aan de verkeerde leverancier gestuurd zijn zal kleiner zijn dan wanneer de gegevens bij een onbekende onbevoegde terecht komen. Er dient tevens rekening gehouden te worden met de duur van de eventuele gevolgen.

5. Bijzondere kenmerken van de persoon (bijvoorbeeld kinderen of andere kwetsbare personen)

6. Bijzondere kenmerken van de verwerkingsverantwoordelijke (aard, rol en activiteiten)

Wanneer er een datalek plaatsvindt bij een medische organisatie zal er een grotere dreiging zijn voor personen dan wanneer de mailingslijst van een commerciële organisatie uitlekt.

7. Het aantal getroffen personen.

¹³ Art. 34 onder 4 AVG.

7. Verantwoordingsplicht en registratie

Ongeacht of een inbreuk aan de toezichhoudende autoriteit en/of de betrokkenen moet worden gemeld, zal deze altijd intern gedocumenteerd moeten worden. Er zijn een aantal elementen die moeten worden opgenomen in de registratie:

- De feiten omtrent de inbreuk;
- de gevolgen daarvan; en
- de genomen corrigerende maatregelen.

De toezichthouder kan inzage verlangen in deze documentatie, het is daarom belangrijk dat de documentatie adequaat is. Zo kan de toezichthouder controleren of datalekken daadwerkelijk gemonitord en opgevolgd worden.

Het is niet verplicht om ook de redenen van het al dan niet melden aan de toezichthouder te documenteren, dit is echter wel aan te raden. Met name wanneer de inbreuk niet wordt gemeld moet de motivering van dit besluit worden vastgelegd.

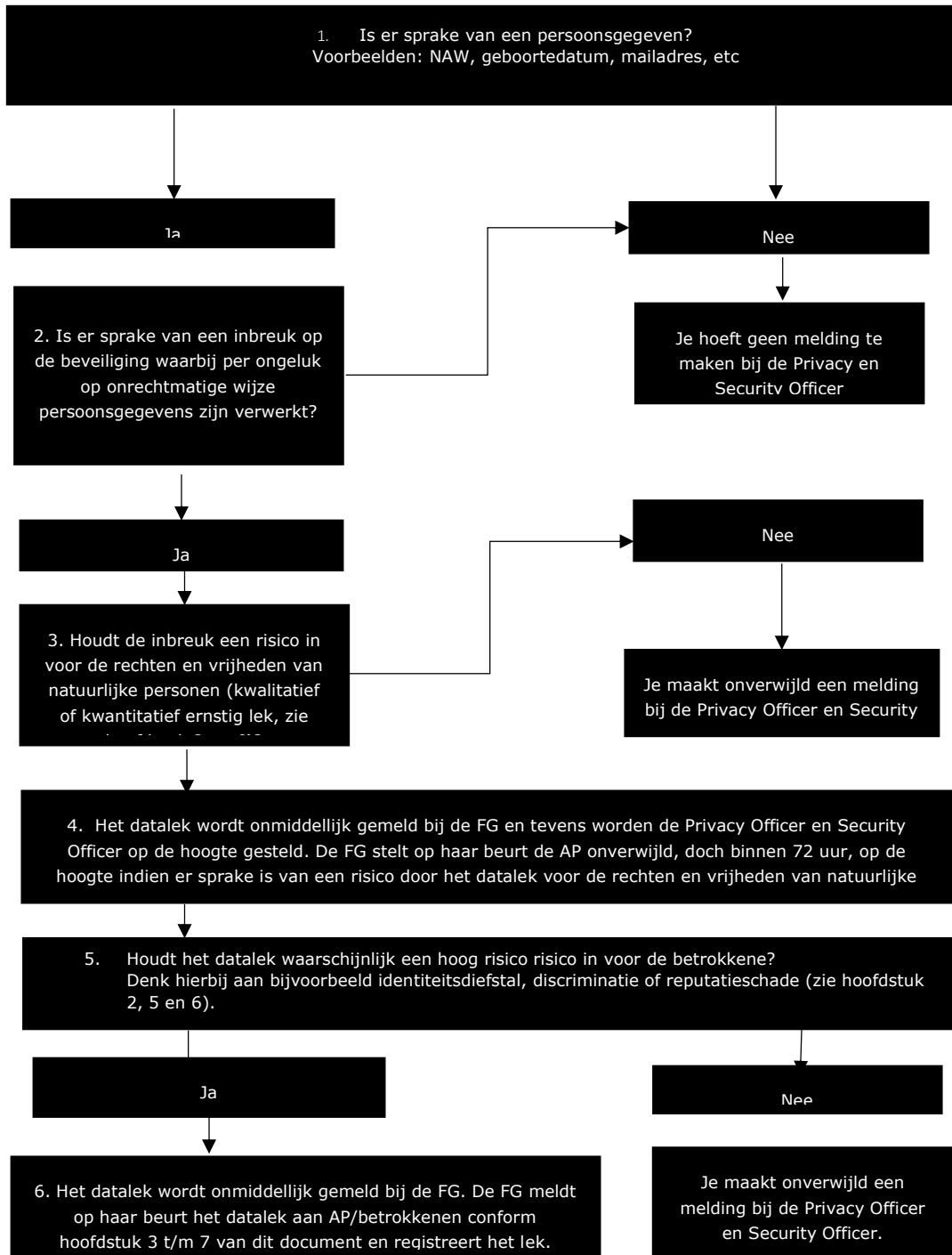
De AP heeft een lijst met tips gepubliceerd voor een goede registratie van een datalek.¹⁴ Deze worden hieronder uiteengezet:

1. Omschrijf incidenten, gevolgen en corrigerende maatregelen duidelijk en volledig;
2. maak een duidelijk onderscheid tussen corrigerende en preventieve maatregelen;
3. maak één overzichtelijke registratie die altijd tot op hetzelfde inhoudelijke detailniveau wordt ingevuld;
4. neem per incident op of, indien aangesteld, de FG is geraadpleegd.
5. neem per incident op of het datalek is gemeld bij de AP en betrokkenen en motiveer daarbij waarom dat wel of niet is gebeurd;
6. indien er een mededeling is gedaan aan betrokkenen, bewaar het bewijs van die mededeling en neem dit op in de registratie;
7. instrueer de personen die verantwoordelijk zijn voor het registeren van datalekken;
8. leg vast welke andere organisaties betrokken zijn geweest bij een inbreuk (zoals verwerkers of sub-verwerkers).
9. overweeg datalekken in te delen naar aard, risico en gevolgen, betrokkenen en mogelijke maatregelen;
10. bespreek de datalekregistratie regelmatig met de juiste personen binnen de organisatie.

¹⁴ Autoriteit Persoonsgegevens 2019, "Handreiking verbetering datalekregistratie" te vinden op: [Handreiking verbeteren datalekregistratie | Autoriteit Persoonsgegevens](#), gepubliceerd op 18 maart 2019, laatst geraadpleegd op 17 augustus 2023.

Bijlagen

1. Beslisboom datalek melden



2. Formulier datalekken en incidenten

Advies beveiligingsincident (omschrijving van het incident)

Reg.nr. in datalekregister:

Reg.nr. in zaakstelsel:

Datum melding (tijdspit en melder):

Feiten

Beschrijf wat er is gebeurd, welke data zijn er mogelijk gelekt, waar deed het lek zich voor, en welke actie is er inmiddels ondernomen om eventuele schade zoveel mogelijk te beperken

Datalek?

Bepaal of sprake is van een datalek

Melding aan de Autoriteit Persoonsgegevens en/of betrokkenen?

Een datalek moet door de verwerkingsverantwoordelijke worden gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 lid 1 AVG). Dit risico bestaat als de inbreuk kan leiden tot lichamelijke, materiële of immateriële schade voor betrokkenen.

Bepaal of gelet op de aard, gevoeligheid, omvang en combinatie van persoonsgegevens de inbreuk kan leiden tot een risico voor de rechten en vrijheden van natuurlijke personen. Motiveer de keuze om wel/niet aan de AP en/of betrokkenen te melden.

Advies

Kortom, het privacyteam adviseert om:

1. dit incident wel/**niet** te kwalificeren als datalek;
2. dit datalek wel/**niet** te melden aan de Autoriteit Persoonsgegevens;
3. dit datalek wel/**niet** te melden aan betrokkene;
4. Eventuele aanvullende adviezen

3. Procesbeschrijving

5.1.2.h

4. Template brief melding betrokkene

[NAAM]

[ADRES]

[POSTCODE + WOONPLAATS]

Instituut Mijnbouwschade Groningen

Cascadeplein 10
9726 AD Groningen

Postbus 40009
8004 DA Zwolle

088 – 042 7220

www.schadedoormijnbouw.nl

fg@schadedoormijnbouw.nl

privacy@schadedoormijnbouw.nl

Datum: [DATUM]

Betreft: Melding Autoriteit Persoonsgegevens

Geachte [NAAM],

Met deze brief stel ik u [OPTIONEEL: , als gemachtigde van de heer/mevrouw XXX,] namens het Instituut Mijnbouwschade Groningen (hierna: het Instituut) op de hoogte van een (mogelijke) datalek. Als gevolg daarvan zijn mogelijk persoonsgegevens in handen gekomen van een derde.

Datalek

Het spijt mij u te moeten melden dat per ongeluk [een e-mail/een e-mail met als bijlage een brief/brief/een verkeerde machtiging] door het Instituut is [toegevoegd aan/verzonden naar een [onjuist e-mailadres/onjuist adres/iets anders]]. Dat had niet mogen gebeuren. Ik betreur dit ten zeerste en bied u hierbij mijn oprechte excuses aan. Het Instituut gaat er alles aan doen om dit soort fouten in de toekomst te voorkomen.

Wat is er gebeurd?

[FEITEN]

Als gevolg van deze fout zijn de gegevens mogelijk terecht gekomen bij een ontvanger die hier geen inzage in had mogen hebben. [OPTIONEEL: Niet bekend is of deze persoon de e-mail/brief ook daadwerkelijk heeft ontvangen, geopend en/of gelezen]. Het Instituut heeft na de verzending op [DATUM DATALEK] de ontvanger [OPTIONEEL: diezelfde dag] per [e-mail/telefoon] verzocht om de [e-mail ongelezen te verwijderen/brief retour te sturen] [OPTIONEEL: , maar heeft hierop (nog) geen reactie ontvangen. Mocht het Instituut op een later moment alsnog een reactie ontvangen, dan ontvangt u daarover uiteraard ook bericht].

Melden bij Autoriteit Persoonsgegevens

[UITLEG DATALEK: welke persoonsgegevens, van wie, wat is er fout gegaan]. Daarom heeft het Instituut een melding gedaan bij de Autoriteit Persoonsgegevens. Verder is ook de interne toezichthouder van het Instituut, de Functionaris Gegevensbescherming, op de hoogte gesteld. Het Instituut heeft geen aanwijzingen dat de toezending van de brief een hoog risico oplevert voor de rechten en vrijheden van betrokkenen. [UITLEG WAAROM GEEN HOOG RISICO].

Meer informatie

Ik begrijp goed dat deze brief vragen kan oproepen. Vanzelfsprekend kunt u contact opnemen met het Instituut. Dat kan met 5.1.2.e [REDACTED], per e-mail (ook voor een telefonische afspraak): fg@schadedoormijnbouw.nl.

Hoogachtend,

[HANDTEKENING BESTUURDER]

[NAAM BESTUURDER] [Voorzitter van het bestuur/FUNCTIE] het Instituut

5. Evaluatieformulier Datalekken

Datalekken Evaluatieformulier

Datum van evaluatie: < datum >

Namen van de functionaris gegevensbescherming, privacy officer en security officier:

<naam FG >

<naam PO >

<naam SO >

Algemene informatie (door PO):

1. **Datum en tijdstip ontdekking:** < vul hier de datum en het tijdstip van het datalek in, door wie het lek is ontdekt, >
2. **Beschrijving van het datalek:** < een gedetailleerde beschrijving van het datalek, inclusief welke gegevens (persoons en/of bedrijfsgegevens) zijn betrokken en hoe het is ontstaan >
3. **Type persoonsgegevens:** < gewoon, bijzonder of gevoelig >

Kenmerken van het Datalek (door PO en SO):

Aard van het datalek: < vul hier de aard van het datalek in: verlies van fysieke apparaten (bijv. verloren laptop), ongeoorloofde toegang tot systemen, onbedoelde openbaarmaking (bijvoorbeeld verkeerd geadresseerde e-mail), technisch falen (bijv. database datalek, social engineering (bijv. phishing), anders namelijk: >

Schaal van het datalek: < vul hier de schaal van het datalek in: klein (slechts enkele records betrokken), matig (tientallen tot honderden records betrokken), groot (duizenden records betrokken), massaal (tienduizenden records betrokken) >

Ernst van het datalek: <vul hier de ernst van het datalek in: verwaarloosbaar (geen tot minimale impact betrokkene), laag (beperkte potentiële schade), matig (potentiële schade, maar beheersbaar), hoog (aanzienlijke potentiële schade), zeer hoog (ernstige langdurige schade en gevolgen voor betrokkenen en organisatie)

(Voorgestelde) maatregelen en opvolging (door PO, SO en FG):

Stappen ondernomen na ontdekking: <vul een beschrijving van de acties die direct zijn ondernomen na het ontdekken van het datalek>

Impactbeoordeling: <vul hier de gevolgen van het dataleke in voor betrokkenen: juridische schade, financiële schade, reputatieschade of andere vorm van schade en/of andere gevolgen>

Voorgestelde maatregelen om toekomstige datalekken te voorkomen: < vul hier de maatregelen in die toekomstige soortgelijke datalekken kan voorkomen >

Ondertekening:

De Privacy Officer, Security Officer en Functionaris Gegevensbescherming stellen hiermee de stand van het datalek vast en formaliseren deze evaluatie:

Handtekening PO, Handtekening SO en Handtekening FG

Jaar
2019

Dataleknr.
5.1.2.e

Getroffen maatregelen (corrigerende of preventieve)

2019	<p>Laptop is goed beveiligd. Eigendom van KPMG. KPMG heeft een melding gedaan richting AP + het datalek geregistreerd. Het incident is bij de AP geregistreerd onder meldingsnummer is 5.1.2.e</p> <p>De laptops van KPMG zijn standaard voorzien van encryptie van de harde schijf en de BIOS. KPMG kan niet met zekerheid vaststellen of er niet meer is ingelogd op de laptop, maar de kans is erg klein.</p> <p>De werknemer heeft direct nadat hij/zij zag/hoorde dat de laptop uit de auto is gestolen zijn/haar account geblokkeerd. Echter, als men het wachtwoord weet, kan er nog wel offline worden ingelogd, zonder dat dit geregistreerd wordt in de online database. Werknemer heeft echter aangegeven dat er niemand is die zijn/haar wachtwoord kan kennen en dat het wachtwoord ook niet ergens geschreven stond bij de laptop. Tot slot is TCMG niet in staat om een laptop op afstand te wipen. Wel is het zo dat alle gegevens voorzien zijn van encryptie, waardoor deze zonder wachtwoord onbenaderbaar zijn.</p> <p>TCMG heeft ook een melding richting AP gedaan. Daarnaast zijn de betrokkenen (MT leden en commissie leden) geïnformeerd over het incident. Organisatorische maatregelen: bewustwording onder MT en commissie leden brengen. Daarnaast geeft medewerker aan dat hij/zij papierloos gaat werken.</p>
2021	<p>Verzoek bij 5.1.2.e ingediend om het fout gekoppelde document te verwijderen uit het dossier van onbevoegde.</p>
2021	<p>Verder melding gemaakt van het datalek bij de AP. En betrokkene(n) over het datalek geïnformeerd.</p>
2021	<p>Verzoek bij 5.1.2.e ingediend om het fout gekoppelde document te verwijderen uit het dossier van onbevoegde.</p>
2021	<p>Verder melding gemaakt van het datalek bij de AP. En betrokkene(n) over het datalek geïnformeerd.</p>
2021	<p>Foutieve documenten uit dossiers onbevoegde gehaald.</p>
2021	<p>Onderzoek afgerond IT-afdeling.</p>
2022	<p>Functioneel beheer voert technisch onderzoek uit en neemt de nodige maatregelen om te voorkomen dat dit soort incidenten in de toekomst voorkomen worden. Privacy heeft een analyse uitgevoerd. Daarbij een melding gedaan van het datalek bij de AP.</p>
2022	<p>Functioneel beheer voert technisch onderzoek uit en neemt de nodige maatregelen om te voorkomen dat dit soort incidenten in de toekomst voorkomen worden. Privity heeft een analyse uitgevoerd. Daarbij een melding gedaan van het datalek bij de AP.</p>
2023	<p>De geadresseerde is verzocht om de e-mail met het verweerschrift en de indiening van het verweerschrift te verwijderen. Hoewel er een tal van persoonsgegevens in het verweerschrift staan (namen burgers, dossiernummers, namen deskundigen, financiële vergoeding beslissing op aanvraag / beslissing op bezwaar), zijn dit voornamelijk gewone persoonsgegevens. De financiële gegevens uit de bip en bob zullen uiteindelijk ook in de uitspraak van de rechtbank worden genoemd en</p>
2023	<p>Brief is vernietigd doc 5.1.2.e. Hoewel er bijzondere persoonsgegevens in het dossier staan zijn deze van algemene strekking. Het risico lijkt ons daarom</p>
2023	<p>verwaarloosbaar. Na intern overleg FG toch gemeld bij AP.</p>
2023	<p>Het bezwaarschrift is verwijderd uit het verkeerde dossier. Het was een handmatige fout, dus er zijn verder geen maatregelen genomen.</p>
2023	<p>De synchronisatie van aanvrager x naar aanvrager y is niet goed gegaan. Functioneel Beheer heeft deze synchronisatie getriggerd en als het goed is, is dit nu</p>
2023	<p>ongelost.</p>
2023	<p>Er is verzocht om het document te verwijderen en tevens verzocht om de post versie te vernietigen.</p>
2023	<p>Op 10 juli 2023 heeft functioneel beheer het verkeerd gekoppelde document verwijderd uit het dossier.</p>
2023	<p>De medewerker die de lijsten heeft verzonden heeft ontvangers verzocht deze definitief te verwijderen.</p>
2023	<p>Document is op verzoek direct uit het dossier gehaald en door de onbevoegde ontvanger verwijderd</p>
2023	<p>Document is op verzoek direct uit het dossier gehaald en door de onbevoegde ontvanger verwijderd</p>

Datalek

Het team Privacy en Informatiebeveiliging krijgt geregeld vragen over de beveiliging van persoonsgegevens en hoe je een datalekkent kunt voorkomen. Voor iedereen is het dan ook goed om te weten wat een datalek is, en wat je moet doen als gegevens eens onbedoeld in andere handen vallen.

Wat is een datalek?

De AVG definieert een datalek als volgt: *“Een datalek is een inbreuk op de beveiliging van persoonsgegevens in digitale of papieren vorm. De inbreuk leidt per ongeluk of op onrechtmatige wijze tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot persoonsgegevens. Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon wordt gerekend tot persoonsgegevens.”*

Kort gezegd gaat het bij een datalek om een inbreuk op persoonsgegevens.

Zo'n inbreuk kan vervelende gevolgen hebben voor de personen waarvan gegevens worden verwerkt. Er is al sprake van een datalek als er gegevens verwijderd of gestolen worden. Of als je per ongeluk een dossier van een aanvrager naar een andere aanvrager stuurt of verkeerd koppelt in BAS of MIRA.

Als je niet zeker weet of iets een datalek is, kun je onderstaand schema gebruiken:

Voorbeelden van een datalek

- een onbevoegde heeft persoonsgegevens van een betrokkene mogelijk gezien, gewijzigd of ontvangen;
- er zijn bestanden met persoonsgegevens verloren of vernietigd en er is geen reservekopie;
- er zijn bestanden met persoonsgegevens mogelijk aangetast door bijvoorbeeld een update of virus (corrupt);
- een harde schijf, USB-stick of dossiers met daarop een kopie van het persoonsgegevens is gestolen of verloren;
- het systeem van een bedrijf dat gegevens verwerkt wordt aangevallen door hackers en de gegevens worden versleuteld (een “ransomware-aanval”);
- iemand stuurt onbedoeld een e-mail met persoonsgegevens door naar een derde;
- iemand stuurt een e-mail naar ontvangers in het veld “Aan” of “CC” in plaats van “BCC”, waardoor elke ontvanger de contactgegevens van de andere ontvangers ziet;
- iemand stuurt persoonsgegevens naar een verkeerde mailinglijst, waardoor de ontvangers onbedoeld toegang krijgen tot de persoonsgegevens;

- een bedrijf dat gegevens verwerkt verliest door een technische complicatie tijdens het updaten van de systeemsoftware een deel van het gegevensbestand, terwijl er geen back-ups zijn.

Wat moet je doen bij een datalek?

Verstuurt iemand per ongeluk iets aan de verkeerde ontvanger? Of maakt iemand een verkeerde koppeling in BAS of MIRA? Dan is er dus sprake van een datalek. Krijg je een melding of maak je zelf een fout? Meld het meteen als je denkt dat er sprake is van een datalek. Volg dan het stappenplan hieronder.

1. Stuur een e-mail naar het team Privacy en Informatiebeveiliging privacy@schadedoormijnbouw.nl met een omschrijving van de volgende punten:
 - Geef aan om wat voor soort document het gaat. Gaat het om iets anders dan een 'standaard' adviesrapport of beslissing, probeer dan kort aan te geven wat de inhoud is en geef aan of het document (bijzondere) persoonsgegevens bevat;
 - Geef aan wanneer het document verstuurd of gekoppeld is;
 - Geef aan wanneer de inbreuk (datalek) plaatsvond;
 - Geef aan wie de ontvanger is, inclusief dossiernummer (BAS of MIRA);
 - Geef aan wie de betrokkene is, en van welk dossier het document onderdeel is, inclusief dossiernummer;
 - Indien bekend: Geef aan of het document verstuurd is door ons (Serviceloket/AOS afdeling) of door de drukker (Xerox).
2. Neem contact op met de ontvanger. Bedank hem/haar voor het doen van de melding, en verzoek om het document ofwel naar ons terug te sturen, ofwel te vernietigen.
3. Mail functioneel beheer met de vraag om het foutief gekoppeld adviesrapport/document uit BAS of MIRA te verwijderen.

Wat doet het team Privacy en Informatiebeveiliging?

Het team Privacy en Informatiebeveiliging wil natuurlijk zo snel mogelijk het datalek oplossen, en maatregelen treffen om ervoor te zorgen dat het datalek niet nog een keer gebeurt. Ook voeren ze administratieve handelingen uit:

- Elk datalek intern registreren in een datalekregister. Wanneer nodig neemt het team contact met je op voor aanvullende informatie.
- Is er een risico voor de betrokkene(n)? Dan melden we het datalek bij de Autoriteit Persoonsgegevens (AP).
- Is er een hoog risico voor de betrokkene(n)? Dan melden we het datalek ook aan hen.

Wanneer moeten we een datalek melden aan de betrokkene(n)?

Als een datalek een hoog risico heeft voor de rechten en vrijheden van betrokkene(n), melden we het datalek dus zo snel mogelijk aan de Autoriteit Persoonsgegevens en de betrokkene(n).

Er is sprake van een hoog risico, als het lek waarschijnlijk het privéleven van betrokkenen kan schaden. Voorbeelden van deze schade zijn bijvoorbeeld identiteitsfraude, discriminatie en reputatieschade. Om goed af te wegen wanneer we wel of niet een melding maken, gebruiken we het stroomschema hieronder.

Wat doe je bij een datalek?

Afgelopen weken lazen jullie het al op PLEK of in de media: het Loket Bevingsschade maakte misbruik van een datalek bij het IMG. Gelukkig is dit lek nu gedicht en zetten we stappen om deze problemen te voorkomen. Ook krijgt het team Privacy en Informatiebeveiliging geregeld vragen over de beveiliging van persoonsgegevens en hoe je een datalekken kunt voorkomen. Daarom is het goed om te weten wat een datalek is, en wat je moet doen als gegevens eens onbedoeld in andere handen vallen. We zetten het voor je op een rij.

Wat is een datalek?

De AVG definieert een datalek als volgt: *“Een datalek is een inbreuk op de beveiliging van persoonsgegevens in digitale of papieren vorm. De inbreuk leidt per ongeluk of op onrechtmatige wijze tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot persoonsgegevens. Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon wordt gerekend tot persoonsgegevens.”*

Kort gezegd gaat het bij een datalek om een inbreuk op persoonsgegevens.

Zo'n inbreuk kan vervelende gevolgen hebben voor de personen waarvan gegevens worden verwerkt. Er is al sprake van een datalek als er gegevens verwijderd of gestolen worden. Of als je per ongeluk een dossier van een aanvrager naar een andere aanvrager stuurt of verkeerd koppelt in BAS of MIRA.

Als je niet zeker weet of iets een datalek is, kun je onderstaand schema gebruiken:

Wat moet je doen bij een datalek?

Verstuurt iemand per ongeluk iets aan de verkeerde ontvanger? Of maakt iemand een verkeerde koppeling in BAS of MIRA? Dan is er dus sprake van een datalek. Krijg je een melding of maak je zelf een fout? Meld het meteen als je denkt dat er sprake is van een datalek, door te mailen naar privacy@schadedoormijnbouw.nl. Bekijk [5.1.2.h](#) voor voorbeelden en het hele stappenplan.

Datalek? Meld het direct.

De afgelopen weken heeft het team Informatiebeveiliging en Privacy (hierna: IB & P) een aantal datalekken moeten melden bij de Autoriteit Persoonsgegevens. Een lek dient gemeld te worden bij de Autoriteit Persoonsgegevens (hierna: AP) binnen 72 uur nadat het bekend is geworden bij ons als organisatie. Het valt ons de laatste tijd op dat de datalekken veel te laat bij ons als IB & P wordt gemeld, waardoor de 72 uur termijn van de AP ruimschoots is overschreden.

Dit is zeer vervelend voor de persoon van wie de persoonsgegevens zijn gelekt. In één geval is er een BSN in combinatie met NAW-gegevens en bedrijfsgegevens van de desbetreffende persoon gelekt. Met deze gegevens kan de ontvanger gemakkelijk fraude plegen. Een BSN wordt daarom ook als een gevoelig persoonsgegeven beschouwd. Hoe eerder de persoon van wie de gegevens zijn gelekt op de hoogte wordt gesteld des te beter. Dan kan deze persoon maatregelen treffen om de risico's te beperken.

Daarnaast zal dit lek naar alle waarschijnlijkheid de aandacht van de AP trekken. Hierdoor zullen wij mogelijk verantwoording moeten afleggen aan de AP en bestaat er kans op sanctiëring, zoals boetes of een berisping. Dit kan vervolgens leiden tot reputatieschade.

Spoedig melden

Daarom verzoekt IB & P jullie vriendelijk om datalekken zo spoedig mogelijk te melden. Iedereen kan een datalek veroorzaken, een ongeluk zit immers in een klein hoekje. Als dit dan gebeurt wees niet bang en meldt het direct bij privacy@schadedoormijnbouw.nl. Twijfel je of er sprake is van een datalek? Meldt het dan ook direct, liever één onjuiste melding te veel dan het niet melden van een daadwerkelijk datalek.

Definitie datalek

Weet jij niet meer precies wat een datalek inhoudt? Hieronder wordt de definitie van een datalek weer voor je uiteengezet:

De AVG definieert een datalek als volgt: "Een datalek is een inbreuk op de beveiliging van persoonsgegevens in digitale of papieren vorm. De inbreuk leidt per ongeluk of op onrechtmatige wijze tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van, of de ongeoorloofde toegang tot persoonsgegevens. Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon wordt gerekend tot persoonsgegevens."

Inbreuk op persoonsgegevens

Kort gezegd gaat het bij een datalek om een inbreuk op persoonsgegevens. Het betreft een inbreuk op de integriteit, vertrouwelijkheid of beschikbaarheid van persoonsgegevens.

Zo'n inbreuk kan vervelende gevolgen hebben voor de personen waarvan gegevens worden verwerkt. Er is al sprake van een datalek als er gegevens verwijderd of gestolen worden (beschikbaarheid). Denk aan het verliezen van een laptop, usb of ander apparaat met persoonsgegevens. Of als je per ongeluk een dossier van een aanvrager naar een andere aanvrager stuurt of verkeerd koppelt in BAS of MIRA (vertrouwelijkheid), waardoor

een onbevoegde toegang krijgt tot het dossier. Als persoonsgegevens worden gewijzigd en daarmee onjuist zijn, is er ook sprake van een inbreuk (integriteit).

Meldt een (vermeend) datalek daarom direct. Dan kunnen wij als IB & P de juiste acties ondernemen. Wij moeten dit als organisatie samen doen en daarom doet IB & P een beroep op jullie oplettendheid.