Formulier melding datalek

Voor het melden van een datalek vult u onderstaand formulier in. Na invulling kunt u dit formulier als PDF opslaan en als bijlage digitaal zenden naar: PG@hogeraad.nl

Of sturen per gewone post naar:
Hoge Raad der Nederlanden
T.a.v. de Procureur-Generaal
Postbus 20303
2500 EH Den Haag.

Nadat u een melding heeft gedaan, ontvangt u een ontvangstbevestiging met daarin een meldingsnummer. Registreer dit nummer voor verdere communicatie met de Procureur-Generaal bij de Hoge Raad.

0. Over deze melding

Gaat het om een nieuwe of bestaande melding?
0 Nieuw
0 Bestaand, het meldingsnummer is: ……

Op grond van welke regelgeving doet u deze melding?
0 Algemene verordening gegevensbescherming (AVG)
0 Wet justitiële en strafvorderlijke gegevens (Wjsg)

1. Contactgegevens en overige algemene informatie

Over welk onderdeel van de rechterlijke organisatie gaat het?
Naam ……..
Adres ……..

Wie meldt het datalek?
Naam ……..
Functie ……..
E-mailadres ……
Telefoonnummer ……..
Met wie kan de Procureur-Generaal contact opnemen voor nadere informatie over de melding?
0 De melder is contactpersoon
0 Er is een andere contactpersoon, te weten:
Naam contactpersoon ……
Functie contactpersoon ……..
E-mailadres contactpersoon ……..
Telefoonnummer contactpersoon ……..

Was er een andere organisatie betrokken bij de inbreuk?
0 nee
0 ja, namelijk ……

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

……

2. Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend

……

Startdatum van de periode waarbinnen de inbreuk was

……

Einddatum van de periode waarbinnen de inbreuk was

……

Duurt de inbreuk op dit moment nog voort?
0 ja
0 nee

Wanneer werd de inbreuk ontdekt?

…….

Als u de inbreuk later meldt dan 72 uur na de ontdekking, wat is daarvan dan de reden?

……

3. Gegevens over het datalek

Aard van de inbreuk
0 Inbreuk op de vertrouwelijkheid van de gegevens
0 Inbreuk op de integriteit van de gegevens
0 Inbreuk op de beschikbaarheid van de gegevens

Aard van het incident

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

0 Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen

0 Brief of postpakket met persoonsgegevens kwijtgeraakt of geopend retour ontvangen

0 Hacking, malware (bijv. ransomware) en/of phishing

0 Persoonsgegevens bij oud papier gezet Persoonsgegevens mondeling gedeeld met onbevoegde ontvanger

0 Persoonsgegevens nog aanwezig op afgedankt apparaat of op afgedankte gegevensdrager (bijv. USBstick)

0 Persoonsgegevens per ongeluk gepubliceerd

0 Persoonsgegevens van verkeerde klant getoond in klantportaal

0 Persoonsgegevens verstuurd of afgegeven aan verkeerde ontvanger

0 Anders, namelijk: ……

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

4. Persoonsgegevens die betrokken zijn bij het datalek

Persoonsgegevens in het algemeen

0 Naam

0 Geslacht, geboortedatum en/of leeftijd

0 Contactgegevens

0 Toegangs- of identificatiegegevens (bijv. inlognaam, wachtwoord, zaaknummer)

0 Locatiegegevens

0 Onbekend / anders, namelijk: ……

Bijzondere categorieën van persoonsgegevens
0 Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
0 Persoonsgegevens waaruit iemands politieke opvattingen blijken
0 Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
0 Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
0 Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
0 Gegevens over iemands gezondheid
0 Financiële gegevens (bijv. rekeningnummer, creditcardnummer)
0 (Kopieën van) paspoorten of andere legitimatiebewijzen
0 Burgerservicenummer (BSN)
0 Genetische gegevens
0 Biometrische gegevens
0 Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen

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

……

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

0 Werknemers
0 Rechtzoekenden/partijen
0 Advocaten
0 Leerlingen of studenten
0 Minderjarigen
0 Personen uit kwetsbare groepen

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

…….

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

……..
Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

……..

6. Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?
0 ja
0 nee
0 deels, namelijk:…….

Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat dat dan?

……

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd? Geef een zo uitgebreid mogelijke toelichting. Indien u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.

…..

7. Gevolgen van het datalek

Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.
0 Onbevoegden hebben kennis kunnen nemen van de gegevens
0 De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden gebruikt
0 Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt
0 Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties
0 Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen
0 Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen
0 Anders, namelijk ……..

Lichamelijke, materiële en immateriële schade voor de betrokkenen
Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?
0 Discriminatie
0 Identiteitsdiefstal of -fraude
0 Financiële verliezen
0 Reputatieschade
0 Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens
0 Ongeoorloofde ongedaanmaking van pseudonimisering
0 Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen
0 Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen
0 Andere gevolgen, namelijk: ……..

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen
0 Verwaarloosbaar 0 Beperkt 0 Aanzienlijk 0 Zeer groot

8. Vervolgacties naar aanleiding van het datalek

Informeren van de betrokkenen
Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen?
0 Ja
0 Nee
0 Nog niet bekend

Wanneer heeft u het datalek gemeld aan de betrokkenen?

……..

Wanneer gaat u het datalek melden aan de betrokkenen?

……..

Wat is de inhoud van de melding aan de betrokkenen? Geef een letterlijke weergave van het bericht aan betrokkenen

……

Hoeveel betrokkenen heeft u geïnformeerd of gaat u informeren?

……

Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken om de betrokkenen te informeren?

……

Waarom ziet u af van het melden van het datalek aan de betrokkenen?
0 De maatregelen die ik heb getroffen voordat het datalek plaatsvond bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten.
0 Het zou een onevenredige inspanning vergen om iedere betrokkene op individuele basis te informeren.
0 Ik heb na het datalek maatregelen getroffen waardoor het niet langer waarschijnlijk is dat zich daadwerkelijk een hoog risico voor zal doen voor de rechten en vrijheden van de betrokkenen.
0 Anders, namelijk: ……

Licht uw keuze toe

Als het informeren van alle betrokkenen een onevenredige inspanning zou vergen, licht dan toe hoe u door een openbare mededeling of een soortgelijke maatregel de betrokkenen gaat informeren.

……

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

…….

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

……..

Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

…….

Internationale aspecten

Heeft de inbreuk zich voorgedaan in een grensoverschrijdende gegevensverwerking?
0 Ja
0 Nee

Als er sprake is van een grensoverschrijdende gegevensverwerking, om welke landen gaat het dan?
…….

Heeft uw organisatie of bedrijf, het datalek gemeld bij privacytoezichthouders in een of meer andere EU-landen, of gaat u dat nog doen?
0 Ja, namelijk……
0 Nee

Heeft uw organisatie het datalek gemeld bij Europese toezichthouders op andere meldplichten, of gaat u dat nog doen?
0 Ja, namelijk …….
0 Nee

9. Overig

Is naar uw mening deze melding compleet?
0 Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig
0 Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk

Ondertekening

Met de ondertekening verklaart u bevoegd te zijn deze melding te doen en dat de in de melding verstrekte informatie juist is.

Handtekening: Datum: