Formulier Melding datalek

In dit formulier zijn de gegevens opgenomen die gemeld moeten worden aan de Autoriteit Persoonsgegevens indien er sprake is van een datalek.

VV Amsterdam zal, als verantwoordelijke voor het melden van een datalek, bepalen of de melding moet plaatsvinden. We zullen de melder op de hoogte houden van de voortgang van onze kant en verwachten dat ook van de melder.

Nieuwe of bestaande melding

1. Gaat het om een nieuwe of een bestaande melding? (kies een van de opties)
   - Nieuw
   - Bestaand

2. Indien bestaand:
   a. Wat is het nummer van de oorspronkelijke melding?

   b. Wat is de strekking van de vervolgmelding? (kies een van de opties)
      i. Toevoegen of wijzigen van informatie betreffende de eerdere melding
      Namelijk:

      ii. Intrekking van de eerdere melding
      Wat is de reden van intrekking?

Wettelijk kader voor de melding

3. Op grond van welke wettelijke bepaling doet u de melding?
   - artikel 33 AVG (zie bijlage voor de tekst van dit artikel)
   - artikel 11.3a, eerste lid, van de Telecommunicatiewet (zie bijlage voor de tekst van dit artikel)

Algemene informatie en contactpersoon die de melding doet

4. Welk bedrijf of welke organisatie doet de melding?
   a. Naam van het bedrijf of de organisatie
   b. (Bezoek)adres
   c. Postcode
   d. Plaats
   e. KvK-nummer

5. Wie heeft het datalek bij de organisatie onder punt 4 gemeld?
   a. Naam van de persoon

b. Functie van de persoon

c. E-mailadres van de persoon

d. Telefoonnummer van de persoon

e. Alternatief telefoonnummer

6. Is het datalek binnen de organisatie vermeld onder punt 4 ontstaan (of door iemand behorend bij deze organisatie veroorzaakt)?
   a. Ja / nee (doorhalen wat niet van toepassing is)
   b. Indien nee, wat is volgens de melder de locatie van het datalek?

7. Met wie kan de Autoriteit Persoonsgegevens (AP) contact opnemen voor nadere informatie over de melding?
   a. De melder is de contactpersoon
   b. Anders:
      i. Naam contactpersoon
      ii. Functie van de contactpersoon
      iii. E-mailadres van de contactpersoon
      iv. Telefoonnummer van de contactpersoon
      v. Alternatief telefoonnummer van de contactpersoon

Gegevens over het datalek

8. Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest:
   Bijvoorbeeld:
   - USB Stick of laptop is gestolen
   - Persoonsgegevens per ongeluk gepubliceerd
   - Hacking, malware of fishing
   - Persoonsgegevens van het verkeerde lid gepubliceerd in het ledenportal
   - Persoonsgegevens van het verkeerde lid verstrekt aan verkeerde ontvanger
   - Anders, namelijk:

9. Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

10. Vond de inbreuk plaats in een verwerking die is uitbesteed aan een andere organisatie?
    a. Ja / nee (doorhalen wat niet van toepassing is)
    b. Zo ja, aan welke organisatie / (sub-)verwerker:

11. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
    a. Minimaal:

    b. Maximaal:

12. Omschrijf de groep(en) mensen (categorieën) van wie persoonsgegevens zijn betrokken bij de inbreuk.

13. Wanneer vond de inbreuk plaats?
    - Op (datum)
    - Tussen (begindatum periode) en (einddatum periode)
    - Nog niet bekend

14. Wat is de aard van de inbreuk? (selecteer één of meerdere opties)
    - Lezen (vertrouwelijkheid)
    - Kopiëren
    - Veranderen (integriteit)
    - Verwijderen of vernietigen (beschikbaarheid)
    - Diefstal
    - Nog niet bekend

15. Om welk type persoonsgegevens gaat het? (Selecteer één of meer opties)
    - Naam-, adres- en woonplaatsgegevens
    - Telefoonnummers
    - E-mailadressen of andere adressen voor elektronische communicatie
    - Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)
    - Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
    - Burgerservicenummer (BSN) of sofinummer
    - Paspoortkopieën of kopieën van andere legitimatiebewijzen
    - Geslacht, geboortedatum en/of leefwijze
    - Bijzondere persoonsgegevens (bijvoorbeeld over iemands gezondheid, geloof)
    - Overige gegevens, namelijk: (vul aan)

16. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (selecteer één of meer opties)
    - Stigmatisering of uitsluiting
    - Schade aan de gezondheid
    - Blootstelling aan (identiteits)fraude
    - Blootstelling aan spam of phishing
    - Anders, namelijk: (vul aan)

Vervolgacties naar aanleiding van het datalek

17. Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken?

18. En om verdere inbreuken te voorkomen?

19. Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (selecteer één van de opties)
    - o Ja
    - o Nee
    - o Nog niet bekend

20. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen?
    a) Ik heb het datalek aan de betrokkenen gemeld op (datum)
    b) Ik ga het datalek aan de betrokkenen melden op (datum)
    c) Nog niet bekend

21. Wat is de inhoud van de melding aan de betrokkenen?

22. Hoeveel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen?

23. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen?

24. Indien u bij vraag 19 nee hebt geantwoord: waarom ziet u af van het melden van het datalek aan de betrokkenen?
    - o De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
    - o Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (verder invullen)
    - o Anders, namelijk (verder invullen)

Technische beschermingsmaatregelen

25. Waren de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
    - o Ja
    - o Nee
    - o Deels, namelijk: (vul aan)

26. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt, op welke manier is dit dan gebeurd?

Internationale aspecten

27. Heeft de inbreuk betrekking op personen in andere EU-landen?
    - o Ja
    - o Nee
    - o Nog niet bekend

28. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?
    - o Ja, namelijk:
    - o Nee

Vervolgmelding

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